PROGRAMA DE DOCTORADO EN CIENCIAS JURÍDICAS Y POLÍTICAS

UNIVERSIDAD PABLO DE OLAVIDE

TESIS DOCTORAL

LAS DILIGENCIAS DE INVESTIGACIÓN ELECTRÓNICA: EN PARTICULAR EL ACCESO A LOS DATOS ALOJADOS EN LA NUBE

Autor: D. Francisco Javier de Lemus Vara
Director: Prof. Dr. Ignacio Colomer Hernández
Catedrático de Derecho Procesal Universidad Pablo de Olavide (Sevilla)
28 de marzo de 2020.

Índice

Introducción

El objetivo de este trabajo es ofrecer al lector una visión exhaustiva y completa de algunas de las nuevas diligencias de investigación insertadas en la Ley de Enjuiciamiento Criminal, tras la reforma operada por la LO 13/2015, de 5 de octubre. Se descarta un examen completo de todas ellas, porque su elevado número y su heterogeneidad haría perder profundidad al estudio que se emprendiera con dicha intención.

Esta tesis, por lo tanto, se ceñirá al contenido de dos de las nuevas diligencias de investigación: la consistente en el acceso y registro a un dispositivo de almacenamiento masivo de información y la que permite el acceso de modo remoto a un equipo informático. Durante el desarrollo del estudio se procederá a exponer el contenido de estas dos diligencias, su regulación legal, sus requisitos, exigencias, presupuestos generales y especiales, así como sus límites, todo ello como aspectos esenciales de la normativa procesal penal que las regula.

De forma complementaria se intentará dar respuesta a algunas cuestiones que la nueva regulación sobre estos métodos de investigación suscitan, y que no quedan debidamente resueltas en el texto legal. En especial las referentes al registro de datos alojados en la nube. Esta materia viene regulada en la ley, pero plantea algunos interrogantes que merece la pena tratar, con la finalidad de intentar alcanzar alguna conclusión práctica sobre ellos. La atención se dirigirá especialmente a la repercusión que pudiera tener la ubicación material de dichos datos en la competencia jurisdiccional definida territorialmente, cuestión que no queda completamente resuelta en el texto legal.

La reforma operada en la ley procesal penal mediante la promulgación de la Ley Orgánica 13/2015 de 5 de octubre, ha ido dirigida, en buena parte, a regular nuevos métodos de investigación de los delitos, basados, sobre todo, en el empleo de la tecnología y la electrónica. Era una materia de la que se carecía completamente de cualquier directriz legal, habiendo quedado todo lo que tenía que ver con esa cuestión bajo el criterio interpretativo de los tribunales, y muy especialmente bajo la doctrina del Tribunal Supremo.

La regulación que se encuentra ahora en vigor resultaba necesaria, y había llegado a ser requerida de modo inaplazable. Sobre todo porque el monopolio que el Estado tiene del *ius puniendi* exige un severo respeto al principio de legalidad y, en especial, al principio de reserva de ley[1], lo que exige del poder estatal tener prevista en las normas legales que promulga, el modo de limitar los derechos

[1] Vid. GÓMEZ RIVERO, Mª del Carmen, «Principios limitadores del ius puniendi», en, *Nociones fundamentales de Derecho Penal, Parte General.* GÓMEZ RIVERO, Mª del Carmen (Dir). Tecnos Madrid. 2015. Págs. 61 a 64.

de los ciudadanos objeto de investigación. La necesidad de una regulación sobre esta cuestión había sido exigida al legislador español por parte de los tribunales tanto nacionales como extranjeros[2].

Hasta la reforma de la LECrim en esta materia, los métodos de investigación criminal basados en la tecnología no estaban resueltos conforme al avance que los nuevos tiempos requerían. Muchos medios de investigación prescindían de la faceta electrónica, y los que así podrían considerarse, o bien eran insuficientes, o simplemente inexistentes. La razón de tal ausencia en el texto legal puede explicarse por diferentes factores como, por ejemplo, la propia antigüedad del mismo o la insuficiencia de otras reformas anteriores a la de dos mil quince, etc.

En todo caso, y pese a la reforma, sigue pendiente la sustitución de la centenaria regulación procesal penal española por otra más adaptada a los nuevos tiempos y necesidades (mayor agilidad en la instrucción y mayor garantía para el procesado). Los intentos en este sentido no han faltado. De hecho, en ese afán reformador se elaboró buena parte del material legal que hoy está vigente. Muchas de las diligencias de investigación electrónica venían recogidas dentro de un proyecto integral de renovación del proceso penal español, conocido como Código Procesal Penal.

El resultado de la reforma de dos mil quince, parte de la cual es objeto de estudio en esta tesis, es un importante cúmulo de métodos de investigación criminal muy heterogéneo y claramente innovador. Su contenido, diverso y de gran alcance, sirve para dar respuesta a una parcela de la actividad investigadora criminal, la tecnológica, que se encontraba yerma de regulación legal.

El método empleado para realizar el presente estudio parte del análisis del texto legal positivo. También se ha considerado necesario acudir a sus fuentes y a sus antecedentes, así como a la génesis del texto y al debate legislativo que precedió a la misma. Además, se analiza cuál era la situación anterior a su entrada en vigor, examinando en especial como la jurisprudencia exponía el modo de proceder ante situaciones en las que era necesario realizar alguna investigación criminal empleando medios tecnológicos aptos para ello.

El presente trabajo además del examen de las claves estrictamente procesales y de los problemas que se plantean en el registro de datos o archivos alojados en la nube, examina también la regulación que en otros países existe sobre estas mismas cuestiones (principalmente en países de nuestro mismo contexto geográfico y cultural: Iberoamérica y Europa). El estudio de esta materia se

[2] Puede citarse como ejemplo de síntesis de estas advertencias, el discurso que en la audiencia solemne a la apertura del año judicial del Tribunal Europeo de Derechos Humanos efectuada el día 30 de enero de 2015, realizó el Presidente del Tribunal Constitucional, Don Francisco Pérez de los Cobos. Págs., 8, 9, 10 y 11. En dicho discurso se analizan brevemente y se enumeran algunas de las más importantes sentencias del TEDH y del TC en la que se incide en el contenido del extinto artículo 579 LEcrim. Puede consultarse el contenido íntegro del discurso en el enlace web siguiente:
https://www.tribunalconstitucional.es/NotasDePrensaDocumentos/NP_2015_005/DISCURSO_APERTURA_DEL_ANIO_JUDICIAL_DEL_TEDH_30_01_2015.pdf

completa con el examen de la regulación contenida en algunas normas internacionales sobre la investigación tecnológica de delitos, en particular de las emanadas las instituciones europeas.

En segundo lugar, además del contenido que podría darse en llamar como estrictamente normativo de las diligencias de investigación, se analiza en la tesis el dato electrónico como objeto sobre el que recae el interés de los investigadores. Lo que es más reseñable en el caso del empleo de cualquiera de los dos métodos de investigación electrónica que se exponen.

La diligencia de acceso y registro de un dispositivo, sea o no remota, busca acceder, obtener y desentrañar el contenido de los datos alojados en el interior de un dispositivo. Esto justifica exponer cómo es el sistema legal que protege todos esos datos. Además, ello permite introducir un nuevo elemento de estudio como es el de los derechos implicados en las diligencias de investigación tecnológica, pues obtener el acceso a todo el conjunto de datos permite conformar un perfil completo del sujeto que los genera. Ese perfil puede quedar expuesto al conocimiento de terceros, que pueden emplear la información extraída de esos datos para muchos fines, incluidos los ilícitos. Por eso, el perfil conformado por los datos de un sujeto ha llegado a ser reconocida como parte integrante de los derechos fundamentales de los ciudadanos[3] y como tal derecho debe recibir una protección adecuada desde el ámbito Procesal Penal. Junto a dicha dimensión de los datos, conformadora de un perfil personal a proteger, los mismos también sirven como objeto de análisis en el proceso penal y por ello su obtención y estudio permiten también servir para acreditar, aunque fuera solo indiciariamente, la comisión de un delito.

El interés del Estado en la investigación y persecución de los delitos, y la irrenunciable protección de los derechos individuales, exige analizar las normas que permitan coexistir ambas exigencias. De hecho, esta es la razón que justifica la necesidad de realizar un análisis de los distintos derechos fundamentales implicados en la tarea de investigación de los datos informáticos o electrónicos obtenidos tras emplear alguna de las diligencias de investigación electrónica. Esto implica acudir a la legislación que los protege, tanto la nacional, como la europea, ambas recientemente modificadas. Se trata de un aspecto que soporta implicaciones tanto de orden constitucional como estrictamente procesal.

La coexistencia en el mismo plano de estudio tanto de las dos diligencias elegidas como de los datos que se obtienen tras su aplicación, exige alguna reflexión más, que también se plasma en este estudio.

[3] Pese a que se abordará este asunto más adelante, y se tratará el derecho al propio entorno digital, procede citar aquí expresamente el fundamento quinto de la STS 489/2018, de 23 de octubre de 2018. Pte: Don Antonio del Moral García. En dicho fundamento ya se expone, en su apartado final que legislativamente se ha considerado que la pluralidad de derechos afectados en el registro de un dispositivo le otorga la necesidad de un tratamiento «*unitario a los datos contenidos en los ordenadores….., configurando ese derecho constitucional de nueva generación*»

La regulación de las diligencias de investigación electrónica permite el empleo de la tecnología para la investigación criminal, y lo hace acudiendo a cuantos medios existen en la actualidad para ello. Sirvan de ejemplo a lo anterior, y se avala así la heterogeneidad de medidas insertas por el legislador en la norma positiva, las diligencias que se refieren a la intervención de teléfonos móviles; la de uso de dispositivos de geolocalización que se pueden colocar en cualquier parte para conocer el paradero del sujeto; el empleo de instrumentos que sirven para grabar conversaciones efectuadas a distancia, o el de cámaras de diverso tipo para grabar las más diversas acciones, etc. Hoy en día es imposible pensar en todos estos actos sin usar algún dispositivo tecnológico.

Las diligencias que se estudian en esta tesis no se apartan en ningún momento de esa naturaleza tecnológica, pues los dispositivos en los que se guarda información son muestra de ella. Pero, puede concluirse que de entre tantas diligencias, estas dos se diferencian de las demás en que son las que más se basan y se centran, casi de un modo exclusivo, en el análisis directo e intensivo en los datos albergados o creados por tales dispositivos.

La finalidad de estas diligencias es extraer directamente del dispositivo-contenedor en el que se ubican, los datos de naturaleza electrónica, y posteriormente analizarlos, traducirlos y ofrecerlos al juez instructor. Por el contrario, en otras diligencias de investigación tecnológica no es tan marcada y evidente esta finalidad, y aunque pueda trabajarse con datos electrónicos, el uso de éstos como objeto de investigación no resulta tan directo.

Por consiguiente, este marcado e intensivo uso de los datos electrónicos se convierte en un rasgo diferenciador y característico de estas dos diligencias. De hecho, puede considerarse que son dos diligencias que se basan en el "uso puro del dato". El dato es creado por el usuario del dispositivo, pero también por algunos aparatos que permiten originarlos, tratarlos, modificarlos y transmitirlos. También esta clase de dato es objeto de búsqueda por los investigadores, para tras el ulterior análisis de su contenido, y de una interpretación de su resultado, pueda servir, o no, como indicio, evidencia o prueba de la comisión delictiva investigada. Los datos se configuran como el objeto que accede a las actuaciones, pero, además, los datos se convierten al mismo tiempo en un objeto de protección. En suma, estas dos diligencias se acaban caracterizando por la intensividad del uso de datos.

En cuarto lugar, en la presente investigación se examina, como ya se ha dicho, de manera separada, la cuestión sobre el acceso y registro a los datos alojados en la nube.

La nube es un tipo de servicio muy extendido, como lo es también casi toda la tecnología, que de una forma o de otra, se describe en la reforma de la LECrim. Pero en el caso de este tipo de

concreto de tecnología se trata de analizar cómo ha abordado la nueva regulación de acceso y registro de dispositivos el modo de hacerlo cuando se trata de "la nube" de un investigado. La respuesta que ofrece la ley a esta pregunta es un tanto equívoca y difusa. Tal indefinición puede dar lugar a ideas confusas, lo que choca con importantes principios procesales generales[4].

Los problemas que plantea el servicio en la nube (*cloud*) no son simples de resolver. En especial surgen dudas en materias de tanta importancia como la competencia del juez instructor para ordenar el acceso, la competencia territorial por la ubicación de esos datos, las nuevas facultades de acceso a Policía Judicial y Ministerio Fiscal (incluido el nuevo Fiscal Europeo) para tomar esa información de forma urgente y apremiante, etc. Estas dudas son de aplicación a las dos diligencias que se tratan en esta obra. La lectura de nuestras normas permite considerar que el legislador ha resuelto esta cuestión, pero sin abarcar todas las situaciones posibles.

Esta materia se aborda mediante la exposición de la competencia territorial, y se exponen las consecuencias de la inobservancia de las normas procesales sobre estas cuestiones. Además, se tratan los mecanismos que existen para poder atajar los defectos en que se hubiera incurrido durante la realización de alguno de estos medios de investigación.

Por último, en quinto lugar, se realiza una exposición sobre cómo debe interpretarse, valorarse y contrarrestarse el resultado que se hubiera obtenido de la práctica de estas diligencias de investigación.

El método empleado para hacer este trabajo, como ya más arriba se ha dicho, parte del estudio y del análisis de las normas legales que regulan estas materias. En este apartado he acudido a las normas nacionales y también le he prestado la necesaria atención a las normas derivadas del Derecho de la Unión Europea. Estas normas de la UE son las que, cada vez con mayor frecuencia, van marcando el camino de las instituciones procesales que guardan intima relación con el uso de las nuevas tecnologías de la información. Esto se debe a que estas instituciones están cohonestadas con el debido respeto a los derechos fundamentales contenidos en los Tratados Europeos, y que son comunes a todos los ciudadanos de nuestro entorno.

El análisis de la legislación se complementa con el que a su vez se deriva del parecer de los Tribunales de Justicia, en especial, la doctrina de la Sala Segunda del Tribunal Supremo, los pareceres del Tribunal Constitucional, y del Tribunal Europeo de Derechos Humanos. El trascurso

[4] En especial será objeto de estudio cómo puede afectarse el principio de competencia territorial que está predeterminado legalmente. La intangibilidad de los datos puede tentar a acceder al ordenador de modo que nos permita a acceder a los datos que alberga, pero cuando se carece de la posibilidad de acceder a ellos más allá de la ausencia de una autorización judicial o porque el dispositivo lo permita, se abren importantes consecuencias relacionadas con la territorialidad y que determinan el modo de acceso a estos datos. Por otra parte, se considera necesario acudir a los mecanismos de cooperación judicial, sobre todo internacionales, cuando ello sea necesario.

del tiempo va aportando una cada vez más consolidada doctrina de la Sala Segunda del Tribunal Supremo sobre el contenido de la nueva ley. También se han incluido resoluciones dictadas por Audiencias Provinciales, que en algunos casos descienden a los problemas que se estudian en este trabajo.

Para el desarrollo de la presente investigación la opinión de la doctrina científica ha sido un instrumento esencial a la hora de interpretar, los no siempre fáciles, términos de los preceptos de la reforma de la LO 13/2015. De hecho, se encuentran autores que se hacen eco de algunos de los problemas prácticos estudiados en este trabajo, principalmente de las relacionadas con la afectación de derechos fundamentales, la protección de los datos de terceras personas que acceden a las actuaciones procesales, la competencia territorial cuando se registran datos en la nube, etc.

El carácter jurídico de este trabajo no impide que se aporten también de modo breve y de forma complementaria, mediante notas al pie, algunas noticias de prensa, artículos y publicaciones en las que puede apreciarse la importancia social y económica del uso y empleo de los datos personales[5].

En resumen, puede decirse que el contenido de la tesis se dirige a estudiar dos aspectos esenciales. Por una parte, el contenido de dos diligencias de investigación: la referente al registro de dispositivos electrónicos y la relativa al examen remoto de equipos. Por otro lado, se analizan, en el seno de ambas diligencias, las implicaciones jurídicas del acceso y el examen de los datos electrónicos cuando estos se encuentran albergados en la nube. Este segundo punto se analiza desde un punto de vista normativo, y se dirige a responder la pregunta siguiente: ¿está correctamente resuelto el modo en que se dispone en la ley este examen de datos contenidos en la nube?, y en caso de que así sea, ¿lo está en todas las situaciones que la práctica presenta?

El registro y análisis de datos en la nube es una materia reciente. De hecho, la aplicación práctica de las nubes digitales constituye algo a lo que todavía nos estamos acostumbrando. Por eso creo que todas sus aplicaciones jurídico-prácticas no se han visto agotadas, incluidas las que puedan tener alguna relación con el ámbito penal sustantivo y procesal penal, y es por esto que, bajo mi personal punto de vista, se trata de una cuestión que aún debe evolucionar y desarrollarse, y lejos de haber agotado toda la problemática que puede presentar, creo que tendrá mucho recorrido jurídico en los próximos años.

[5] Con la finalidad de mostrar la cada vez más importante dimensión social que los datos electrónicos tienen hoy día, el lector puede encontrar referencias a noticias de actualidad, extraídas de diversos medios de comunicación de masas, en notas al pie de página, que aluden y tratan sobre la importancia social y económica que los datos electrónicos presentan en la sociedad contemporánea. Con ello se busca ofrecer una pincelada que permita vislumbrar que el uso de datos electrónicos está más allá de lo jurídico.

1. Los datos electrónicos como objeto de investigación criminal. Implicaciones constitucionales.

1.1. La protección constitucional de los datos electrónicos.

La evolución tecnológica experimentada en las últimas décadas del S XX y primeras del actual, aporta evidentes ventajas que no es necesario explicar, pero, como contrapartida, también provoca importantes controversias y problemas de indudable interés jurídico.

La relevancia jurídica que presenta el empleo de la tecnología se manifiesta en muchos frentes: la influencia de la edad de las personas que emplean estos instrumentos y servicios tecnológicos y digitales, como los menores de edad[6]; su uso en el ámbito civil (como por ejemplo en la contratación a través de medios electrónicos[7]), en el ámbito laboral (lo que se constata con el uso de las tecnologías para controlar el desempeño laboral, o como causa de conflictos de esta naturaleza[8]) o en el contencioso administrativo (con la creciente presencia de la Administración en la red, generando al ciudadano que disponga de medios digitales para recibir notificaciones[9]).

El ámbito penal también es otro orden en el que destacan problemas derivados del uso de las nuevas tecnologías (el uso de internet y el empleo de los medios de comunicación y su difusión electrónica, son tanto medios de comisión delictiva como fórmulas que permiten su investigación). En este ámbito concreto, tanto el uso de dispositivos, como el de los datos generados por ese empleo, presentan importancia para el Derecho penal.

La tecnología, su uso, así como los datos que genera, pueden servir como medio para ser indicio de la comisión de un delito y por ello desvirtuar la presunción de inocencia conllevando la imposición de una pena de privación de libertad.

---

[6] Vid. GIL ANTÓN, Ana María. «El menor y la tutela de su entorno virtual a la luz de la reforma del código penal lo 1/2015. Virtual environment and child protection», *Revista de Derecho UNED*, núm. 16, 2015. Pág. 275 y siguientes.

[7] La contratación mediante instrumentos electrónicos, sus efectos y su eficacia, es una cuestión que se regula en la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

[8] Véase en esta materia y a mero título de ejemplo, la STS 119/2018, de 8 de febrero. Ponente: D. Luis Fernando de Castro Fernández.

[9] Véase la STS 47/2018, de 17 de enero. Ponente: D. Nicolás Maurandi Guillen, donde se realiza un estudio sobre la validez de una notificación administrativa realizada por vía electrónica de unas liquidaciones tributarias.

Por consiguiente, se debe permitir investigar su uso en el más amplio sentido. El acceso a estos aparatos, a su contenido, a los datos que albergan, e incluso a los que se han transmitido y todo su estudio posterior se convierten en un modo apto para descubrir a los responsables de los delitos. Estos datos pueden también ser útiles para acreditar hechos relacionados con otras personas que están siendo investigados, conocer quienes son las víctimas, etc.

La utilidad de la tecnología en las actividades de persecución de delitos es fuente de importantes controversias, siendo las más habituales las derivadas de la fuerte limitación que experimentan algunos derechos fundamentales para la obtención de estos datos.

La finalidad perseguida en la reforma de la LECrim ha sido conciliar la finalidad de investigación de los delitos con la tutela de los derechos fundamentales, estableciendo el modo en que pueden llevarse a cabo las limitaciones a tales derechos, en concreto a los derechos del art. 18 CE. Con el establecimiento de esta regulación se refuerzan a estos derechos con las garantías necesarias para su protección, y al mismo tiempo se fortalece el propio proceso penal, pues el seguimiento de estas normas de limitación evita la exclusión de su contenido de la investigación por la concurrencia de una indeseable nulidad.

Lo primero que ha de destacarse es que las diligencias contenidas en los arts. 588 sexies y 588 septies LECrim, que irán siendo objeto de exposición, sólo pueden afectar al contenido de los derechos que se enumeran en el art. 18 CE. En el caso específico de estas medidas de investigación, los datos, traducidos del lenguaje informático en el que se encuentran al que nos resulta comprensible, pasan a ser imágenes, textos, documentos, mensajes o llamadas ya realizadas, y los derechos implicados en todos esos formatos son los que se enumeran en alguno de los apartados de ese concreto precepto constitucional.

El nuevo Título VIII de la LECrim contiene una regulación completa y muy detallada de diferentes diligencias. Cada una de ellas sirve para limitar, con las garantías jurídicas adecuadas, los derechos correspondientes a la privacidad e inviolabilidad del domicilio[10], el derecho a que no se desvelen documentos personales que no conforman ningún proceso de comunicación[11], y al derecho al secreto de la correspondencia escrita (y claro está, también la realizada de manera digital) [12]. La nueva ley configura una profusa regulación de la diligencia que limita el derecho al secreto de las

[10] Y ello en la medida en que el Capítulo I (arts. 545 a 572 LECrim) contiene la medida consistente en la entrada y registro en domicilio y otros lugares.
[11] El Capítulo II regula en sus arts. 573 a 578 LECrim una afectación al derecho a la intimidad consistente en el registro de libros y papeles.
[12] El Capítulo III regula en una nueva redacción del art. 579 y 579 bis, así como hasta el art. 588 LECrim lo relativo a la apertura de correspondencia.

comunicaciones telefónicas y telemáticas[13] y sobre la captación de estas comunicaciones empleando los sofisticados medios que la tecnología pone al alcance de los investigadores para obtenerlos de manera distinta al mero "pinchazo telefónico"[14]. La nueva norma cuenta incluso con diligencias que afectan a distintas acepciones del derecho a la intimidad como la consistente en autodeterminar el lugar en el que alguien se encuentra en el espacio sin que los demás tengan porqué saberlo[15], etc.

En el caso concreto de las dos diligencias de acceso, extracción y registro de información digital contenida en dispositivos electrónicos, cabe decir que son, de entre todas las que se contienen en el Título VIII LECrim, las más proclives a afectar de forma simultánea a varios de los derechos constitucionales del art.18 CE.

Con carácter general puede decirse que las diligencias de investigación que se contienen en el Título VIII ya mencionado, van refiriéndose, una a una, a derechos constitucionales muy concretos, con contornos perfectamente precisados, deslindados y delimitados, pero en el caso de las diligencias de los arts. 588 sexies y septies LECrim se quiebra la perfecta correspondencia con un derecho concreto, que no está tan clara y precisada como en el caso de las demás.

Por ejemplo, si el derecho al secreto de la correspondencia tiene previsto el modo de limitarse mediante la diligencia de apertura de correspondencia escrita, o si el secreto de las comunicaciones cuenta con una diligencia de intervención específica para eso, o si el derecho a la inviolabilidad del domicilio lo hace con la regulación de la diligencia de entrada y registro, no pasa lo mismo con estas diligencias de acceso y registro de dispositivos.

La difuminación de los distintos derechos afectados por estas diligencias se debe a la distinta clase de información que se puede encontrar en un artefacto electrónico, así como a las distintas y variadas operaciones que pueden hacerse con ellos. Tantas funciones y actividades permiten que se afecten a varios derechos al mismo tiempo[16]. Por ejemplo, los correos electrónicos que aún no han sido leídos y que se encuentran en un ordenador intervenido de modo remoto, pueden afectar al derecho al secreto de las comunicaciones; en cambio, los correos electrónicos ya generados y leídos pueden lesionar, en caso de accederse a ellos de manera indebida, afectan al derecho a la intimidad, lo que se extiende además también a videos y documentos que pudieran albergarse en el interior del

[13] El Capitulo V en sus arts. 588 ter a, hasta el art. 588 ter m, regulan el modo de intervenir estos procesos de comunicación.
[14] El Capítulo VI regula en los arts. 588 quáter a hasta el art. 588 quáter e, el modo de realizar la captación de comunicaciones orales empleando medios tecnológicos aptos para ello.
[15] El Capítulo VII regula en sus arts. 588 quinquies a, hasta el art. 588 quinquies apartado c, un tipo de diligencia de investigación electrónica que permite conocer y seguir el paradero de una persona, mediante la colocación de balizas y dispositivos similares, aptos para ello.
[16] La STS 489/2018, de 23 de octubre de 2018. Pte: Don Antonio del Moral García dispone, citando la STS 342/2013, de 17 de abril, que entre tales actividades están el uso de mensajes, el tratamiento de imágenes, la redacción de documentos o el empleo de correos electrónicos.

dispositivo que se encontrase. Pero incluso más allá, los datos derivados de la propia participación del investigado en las redes sociales, el uso que haga de la red internet y su acceso a páginas web, así como los metadatos que reflejan estas operaciones o los resultados de compras realizadas on line, son también elementos de interés para la causa que pueden afectar a varios derechos del art. 18 CE al mismo tiempo.

Esta situación aconseja realizar un estudio somero de los derechos fundamentales en general, para, seguidamente, entrar en el contenido de los que pueden verse afectados durante la ejecución de las diligencias de investigación penal de los arts. 588 sexies y septies LECrim, así como analizar cuáles son los medios de protección con los que se los ha dotado por parte del legislador, en especial dentro del ámbito penal, orden en el que gravita el ámbito de las diligencias estudiadas en esta tesis.

1.1.1. Los derechos constitucionales: concepto, rasgos y clasificación.

Las sociedades actuales, y más concretamente, aquellas de corte occidental, se sustentan y se desarrollan en base a las disposiciones que se contienen en sus textos constitucionales. Estos textos, son el resultado de una intensa evolución histórica, política y jurídica. En ellos se esboza la configuración sociopolítica de las sociedades que se rigen por ellas, y se contienen los aspectos básicos y esenciales sobre el modo de organización social elegido, como por ejemplo la forma de elaborar las normas jurídicas o el modo en que se configura la organización territorial del Estado.

Los textos constitucionales, además de lo anterior, también determinan las reglas concretas sobre la aplicación práctica de la división de poderes o el modo de ejercer el derecho a la participación ciudadana en la toma de las decisiones relativas a su propia representación como sociedad en los diferentes poderes del Estado. Además de todo esto el contenido de un texto constitucional también suele realizar una importante enumeración, de indudable interés práctico para los ciudadanos, que es la relativa a los derechos fundamentales.

El concepto de derechos fundamentales se desenvuelve entre lo interiorizado y lo apriorístico[17]. Es una categoría que resulta sencilla de entender y que se refiere a los elementos más esenciales que exige el desarrollo de la vida cotidiana de cualquier individuo[18], compatibilizando esta dimensión

[17] La antigua STC 53/1985, de 11 de abril. Ponentes: Doña Gloria Begué Cantón y Don Rafael Gómez Ferrer Morant, alude a este carácter primario.
[18] De ahí que deban entenderse como aspectos que integran la dignidad de la persona y su libre desarrollo conforme se establece en el art. 10.1 de la Constitución.

intrínseca con la pluralidad y la diversidad propias de las sociedades actuales, así como ejerciendo un claro papel de garantía frente a la actuación del Estado.

La importancia de estos derechos para los ciudadanos debe verse respaldada con el respeto plural de los demás conciudadanos, así como también con su escrupulosa observancia por parte del Estado, en sus diferentes manifestaciones y poderes. En el caso de este último, se necesita, además, un papel activo en orden a tutelarlos y protegerlos de cualquier vulneración.

Precisamente, el notable incremento de todas las dimensiones y actividades humanas, unido a una verdadera toma de conciencia social de las diferentes necesidades individuales, han ido engrandeciendo el número, la extensión, la importancia y el ámbito de aplicación de los derechos fundamentales.

La evolución experimentada por los derechos fundamentales en los últimos tiempos se ha producido, sobre todo, en su faceta más plural, social y colectiva, al estar mucho más consolidada la dimensión individual y liberal, que tradicionalmente han representado algunos de ellos. En todo caso, unos y otros siempre deben ser objeto de especial cuidado y atención.

Este concepto de derechos fundamentales ha evolucionado desde una posición de corte liberal-individual tradicional: la vida, la integridad física, la libertad y la propiedad, a uno mucho más amplio o colectivo, que abarca dimensiones sociales e incluso prestacionales, en la que resulta insoslayable el papel activo del Estado (la prestación de educación, el cuidado y fomento de la cultura, la obligación de proporcionar sanidad o proteger el medio ambiente).

Esto permite afirmar que el concepto de los derechos fundamentales no es estático, fijo e inamovible, sino que sigue en constante replanteamiento, evolución y movimiento.

Los acontecimientos derivados de la importante crisis económica padecida desde el año 2009 sirven de ejemplo. Este evento ha levantado un gran debate social acerca de determinados aspectos de la vida cotidiana de los individuos, muchos de los cuales se entienden y exigen como verdaderos derechos fundamentales[19]. La vitalidad que se ha dado a los derechos de los consumidores frente a grandes compañías mercantiles, son entendidos como aplicables a una suerte de nuevo concepto de ciudadano, que ya no es tanto un sujeto político sino un individuo marcado por la Sociedad actual,

[19] Durante las manifestaciones del movimiento del llamado quince de marzo, se suscitaron diversos debates sobre el derecho a la vivienda y todo lo que de esta cuestión se derivaba, los derechos y facultades que los ciudadanos tienen frente a las empresas de todo tipo, pero en especial los Bancos y entidades financieras. También se plantearon reforzamientos de derechos como la salud, la educación, etc.

bastante mercantilizada, y que se contrapone no ya tanto al concepto de Estado, tradicional invasor de sus derechos, sino al de empresa[20], nuevo agente que amenaza su consideración individual.

Esta exigencia de los ciudadanos instando un mejor y más completo respeto a los derechos recogidos en los textos constitucionales, e incluso la exigencia en una mayor extensión de los mismos que ha recorrido buena parte de occidente se debe a una casi unánime enumeración de estos derechos en las constituciones posteriores a la Segunda Guerra Mundial, donde son recogidos y reconocidos[21], así como su inclusión en algunos textos internacionales que se tornan derecho internacional aplicable[22].

Desde una óptica netamente jurídica, la doctrina encuentra el fundamento de estos derechos en aspectos «*axiológicos, jurídicos y antropológicos»*[23], y los conceptúa como *«aquellos derechos de los que es titular el hombre no por concesión de las normas positivas, sino con anterioridad e independientemente de ellas y por el mero hecho de ser hombre, de participar de la naturaleza humana»* [24]. Otros autores, buscando una definición más práctica, estiman que los derechos fundamentales son «*aquellos derechos humanos garantizados por el ordenamiento jurídico positivo, en la mayor parte de los casos en su normativa constitucional, y que suelen gozar de una tutela reforzada»*[25].

---

[20] A mi juicio, esa es la conclusión que puede extraerse de la observación de los hechos acaecidos en los últimos años, y sobre todo en aspectos, por todos conocidos, como los movimientos sociales del 15-M, la polvareda generada por las hipotecas con cláusulas suelo, las ventas masivas de productos financieros complejos de todo orden, los desahucios derivados de impagos de hipotecas o la sensibilidad social derivada de la pérdida de empleo estable. Son todos ellos aspectos que han influido en el modo de entender al individuo en el arranque de las primeras décadas del siglo XXI, y que ha hecho que los ciudadanos reclamen una nueva parcela de derechos, que entienden como fundamentales. Sólo el tiempo dará respuesta a las reclamaciones efectuadas.

[21] Hay que destacar el contenido del art. 10.2 de la CE conforme al cual *«Las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los tratados y acuerdos internacionales sobre las mismas materias ratificados por España».* Citaremos como normas internacionales esenciales sobre este particular las siguientes: la Declaración Universal de los Derechos Humanos (Declaración de 10 de diciembre de 1948, adoptada y proclamada por la 183.ª Asamblea General de la Organización de las Naciones Unidas). El Pacto Internacional de Derechos Civiles y Políticos de 19 de abril de 1966 (Instrumento de Ratificación de 13 de abril de 1977). El Pacto Internacional de Derechos Económicos, Sociales y Culturales, de 19 de diciembre de 1966 (Instrumento de Ratificación de 13 de abril de 1977). El Convenio Europeo de Derechos Humanos (Instrumento de Ratificación de 26 de septiembre de 1979), y por último la Carta de los Derechos Fundamentales de la Unión Europea.

[22] Como ha señalado lo que se busca principalmente es que *«se pretende convertir en normativa de cualquier ordenamiento jurídico positivo»* (Cfr. AREITIO RODRIGO, Ramón. *Lecciones elementales de Derecho Natural*, Publicaciones de la Universidad de Deusto, 1996. Pág. 45).

[23] Cfr. TORRES DEL MORAL, Antonio. "Fundamento, naturaleza y sujeto de los derechos", en (Gimeno Sendra et. al). *Los derechos fundamentales y su protección constitucional*. 2ª ed., EDISOFER. Madrid. 2017. Pág. 83. Sucintamente considera el autor que el elemento axiológico se refiere a la recogida de valores generalmente considerados como esenciales e imprescindibles por las sociedades, que los consignan en normas jurídicas, lo que le abre la vía al elemento normativo mencionado, y seguidamente, tales valores consignados en normas jurídicas sirven al ciudadano y a sus necesidades.

[24] Cfr. FERNÁNDEZ GALIANO, Antonio y DE CASTRO CID, Benito. *Lecciones de Teoría del Derecho y Derecho Natural*. Editorial Universitas. Madrid. 2001. Pág. 533.

[25] Cfr. PEREZ LUÑO, Antonio E. *Los derechos fundamentales.* Tecnos. Madrid. 2005. Pág. 46.

La definición anterior deja atrás antiguas concepciones doctrinales que entendían a los derechos fundamentales como derechos mas bien programáticos y destinados a influir en el contenido de las leyes que se dictasen sobre esas materias [26].

Esta primera consideración se resolvió concluyéndose con que estos derechos son auténticas normas jurídicas, preceptos de primer orden, y por ello, directamente aplicables y esgrimibles por los ciudadanos ante los tribunales [27]; en suma, la doctrina los considera «*Derecho directamente aplicable»* [28], siendo al mismo tiempo criterios, principios y valores que conforman e inspiran el desarrollo de la Sociedad y la actuación del Estado (art. 1 y 10.1 CE) [29] .

En cuanto a sus características, los derechos fundamentales destacan por su «*imprescriptibilidad*, la *inalienabilidad*, la *irrenunciabilidad* y la *universalidad»* [30], lo que les impide ser derechos sujetos a transacción en la medida en que son inherentes al ser humano[31]. Sus características reflejan su inmanencia y permanencia de manera que se constituyen como un rasgo identificador del ser humano.

En tercer lugar, se destaca la vinculación que estos derechos representan para el Estado, que debe guiarse por su contenido, estando obligado a observarlos, a protegerlos, a fomentarlos y a tenerlos presentes en su actuación de creación y de aplicación normativa[32], pero en todo caso debe respetar

---

[26] No se trata solo de un interrogante propio de nuestra doctrina, sino que se ha planteado en otras latitudes. Véase Vid. MÜLLER, FRIEDRICH. *La posibilidad de los derechos fundamentales: cuestiones para una dogmática práctica de los derechos fundamentales*. Dykinson. Madrid. 2016. Pág. 180. El autor concluye que el Tribunal Federal Alemán ha considerado que los derechos fundamentales consignados en la Carta Magna germana tienen la consideración de verdaderas normas legales.

[27] Vid. SÁNCHEZ GONZÁLEZ, Santiago. «Los derechos fundamentales en la Constitución española de 1978», en SÁNCHEZ GONZÁLEZ, Santiago. *Dogmática y práctica de los derechos fundamentales*. Tirant lo Blanch. Valencia. 2015. Págs. 16 y 17. El autor en las dos páginas hace mención a que los derechos fundamentales contenidos en la Constitución no gozan de una única naturaleza, sino que al mismo tiempo ostenta varias.

[28] Cfr. TORRES DEL MORAL. Op. cit, Pág. 57.

[29] Esta doble naturaleza de los derechos ya ha sido reseñada por el propio Tribunal Constitucional en STC 25/1981, de 14 de julio. Ponente: Don Antonio Truyol Serra. El Fundamento jurídico quinto dispone: *«los derechos fundamentales, que presentan la doble dimensión de derechos subjetivos de los ciudadanos y de «elementos esenciales de un ordenamiento objetivo de la comunidad nacional, en cuanto ésta se configura como marco de una convivencia humana justa y pacífica ...».*

[30] Vid. FERNÁNDEZ GALIANO y DE CASTRO CID. Op. cit. Pág. 537. El autor describe detalladamente cada una de estas tradicionales características que se predican de los diferentes derechos fundamentales, y lo hace en contraposición a las que son propias de los demás derechos subjetivos, que ostentan un carácter patrimonial de menor alcance.

[31] Estas características constituyen, en no pocas ocasiones, elementos que sirven como fundamento a recursos. Se cita como ejemplo la STS 28 de marzo de 2014 en el recurso 292/2013 en el ámbito de lo contencioso administrativo, y en otras muchas, como por ejemplo, la STC 208/2013, de16 de diciembre. Ponente: Doña Adela Asua Batarrita. La sentencia que se pronuncia sobre una constante controversia generada entre el derecho al honor y a la intimidad con respecto al derecho a la libertad de información cita expresamente estas características predicables de los derechos fundamentales.

[32] Vid. TORRES DEL MORAL, Op. cit, Pág. 84-85. Se habla también por el autor de que en ocasiones estos valores actúan como exhortaciones a los poderes públicos. Lo que defiende el autor en el texto es que los derechos constitucionales integran, al mismo tiempo, diferentes alcances, algunos con más trascendencia jurídica que otros. Unos exigibles, otros no tanto.

su contenido, como normas jurídicas que son, en base a lo que dispone el art. 9.1 CE y el principio de seguridad jurídica[33].

Este principio actúa como garantía para los administrados porque pueden saber el modo en que el Estado debe actuar (entiéndase el concepto en el más amplio espectro de poder estatal) ajustando siempre su actuación al mandato de la ley (lo que es una manifestación del principio de legalidad).

En el ámbito propio del proceso penal, donde se desenvuelve el objeto de este trabajo, la protección de los derechos fundamentales debe hacerse compatible con el ejercicio por el Estado del *ius puniendi*. Esto se concretará en que toda la actuación del Estado dirigida a perseguir delitos y a sancionarlos, ha de respetar unos principios que compatibilicen esa función, con el respeto a los derechos fundamentales. Los principios más básicos serían el principio de legalidad penal y procesal, el respeto al derecho a la libertad personal, el derecho a la tutela judicial efectiva, el principio de retroactividad de las normas penales más favorables, el principio *ne bis in ídem*, etc.

Los derechos fundamentales pueden ser clasificados según diferentes criterios. Uno de estos criterios clasificatorios es el que los distingue según el mecanismo de protección que les brinda el texto fundamental[34], otros criterios de diferenciación parten del contenido, de la función o finalidad que persigan: así hay algunos que contemplan la protección de aspectos netamente individuales, otros versan sobre dimensiones colectivas como los «*derechos de participación, derechos económicos*»[35], otros se refieren a deberes, etc. En todo caso, la clasificación más tradicional es la que diferencia entre derechos y libertades individuales[36].

Los derechos con rango constitucional que se verán más afectados por las diligencias estudiadas en este trabajo son el derecho a la intimidad personal y familiar, el derecho a la inviolabilidad del domicilio, el derecho al secreto de las comunicaciones privadas, el derecho a la autodeterminación informativa y el derecho a la identidad digital y algunos aspectos relacionados con la protección de datos[37].

Pese al carácter tradicional que presentan estos derechos, no puede decirse que se trate de figuras jurídicas estáticas, al contrario, parecen experimentar una lenta pero constante evolución y

[33] La STC 46/1990, de 15 de marzo. Ponente: Don Vicente Gimeno Sendra, dictada en pleno, sobre aspectos derivados de una norma dictada por el Parlamento de Canarias, estudia varios de los aspectos que se contienen en el art. 9 del texto constitucional tales como la prohibición de retroactividad de normas no favorables, el principio de seguridad jurídica. En concreto sobre este último determina que una de las funciones del legislador es la de buscar *«claridad y evitar la confusión normativa»*

[34] Cfr. ALZAGA VILLAAMIL, Oscar, GUTIÉRREZ GUTIÉRREZ, Ignacio y RODRÍGUEZ ZAPATA, Jorge. *Derecho Político español, según la Constitución de 1978. II. Derechos fundamentales y órganos del Estado*. Tercera Edición. Editorial Centro de Estudios Ramón Areces. SA. Madrid. 2002. Pág. 43.

[35] Cfr. ÁLVAREZ CONDE, Enrique *Curso de Derecho constitucional*. sexta edición. Madrid. Tecnos. 2008. Págs. 352.

[36] Cfr. ALZAGA VILLAAMIL, GUTIÉRREZ GUTIÉRREZ y RODRÍGUEZ ZAPATA. Op. Cit. Pág. 45.

[37] La STS 489/2018, de 23 de octubre de 2018. Pte: Don Antonio del Moral García, hace alusión expresa en su fundamento quinto a los derechos del art. 18.1, 18.3 y 18.3 CE.

adaptación a las nuevas realidades sociales, destacándose especialmente la irrupción de las nuevas tecnologías. Un ejemplo de la actualización y adaptación a la realidad social de algunos de los derechos constitucionales que se ven afectados por las diligencias de investigación que más adelante se estudiarán, se aprecia en el contenido de la Ley Orgánica reguladora de la protección de datos (LO 3/2018 de 5 de diciembre) y en el reconocimiento de nuevos derechos contenidos en ella como los de acceso, tratamiento, portabilidad, o supresión. La vía normativa no es la única mediante la que se desarrollan estos derechos, sino que la determinación de su alcance y su contenido también se realiza por vía jurisprudencial. Un ejemplo, sobre el que se volverá más adelante, es la creación y el desarrollo del derecho al propio entorno virtual. Este último es un claro ejemplo de cómo se refuerzan, amplían y desarrollan algunos derechos de reconocida raigambre, de manera que se hacen más adecuados a las nuevas realidades tecnológicas que se han convertido en una constante en el mundo de hoy.

La finalidad que ha perseguido la regulación procesal que se analizará a lo largo de esta tesis no ha sido otra, en el caso de las diligencias de registro de datos, que dar una respuesta a la necesidad de conjugar la protección de los derechos fundamentales relacionados con los datos de los individuos, en cualquiera de las dimensiones asociadas a los derechos del art. 18 CE, con la investigación criminal. En el siguiente apartado veremos que la protección de los derechos que menciono no es sólo la procesal, sino que configuran una realidad que recibe tutela desde diversos ámbitos normativos.

1.1.2. La protección jurídica de los derechos con rango constitucional.

Los derechos fundamentales exigen una adecuada protección ante cualquier vulneración de los mismos, para que sean una realidad tangible y efectiva que los aleje de una consideración abstracta.

El conjunto de derechos de un individuo, tanto los fundamentales, como los que no lo son, conforman una globalidad para su titular, susceptible de ser defendida[38]. No hay razón para que los derechos fundamentales no puedan entenderse como una parte de ese acervo de derechos y, por consiguiente, su titular pueda ejercer cualquier acción en su defensa, o si lo desea, omitirla.

[38] Esta concepción tan civilística, propia de la parte general del derecho civil, puede consultarse en muchas obras de esta materia, en especial Vid. ALBALADEJO, Manuel. *Derecho Civil I. Introducción y parte general*. EDISOFER. Madrid. 2013. Pág. 304. Debo matizar que el concepto ha de ser entendido no como la defensa de un patrimonio en el sentido exclusivamente civil, sino que considero que se puede partir de esa concepción aunque abstrayéndola al ámbito de los derechos en general. Esta concepción permite considerar que el ejercicio de la protección de cualquier derecho fundamental forma parte también del conjunto de derechos en general.

La concreta protección de los derechos fundamentales se realiza mediante la implementación de mecanismos específicos creados por el ordenamiento jurídico con ese fin. En lo que interesa a este trabajo, la tutela de los derechos implicados en la práctica de determinadas diligencias de investigación electrónica, están orientados a evitar una exagerada y desmedida intervención del Estado en concretos derechos fundamentales del individuo, que pudieran producirse en el desarrollo de sus legítimas funciones de prevención, persecución y castigo de las actividades ilícitas. Para evitar dicha posibilidad se habilitan concretos medios de control de la actividad investigadora del Estado sometiendo dichos medios a un estricto principio de legalidad, que dote de seguridad jurídica la realización de estas acciones. De manera más concreta será cada norma jurídica que desarrolle por separado cada diligencia de investigación electrónica, la que determine la forma más adecuada de limitar los derechos afectados en cada caso de manera respetuosa con las leyes y con su contenido.

La protección general de los derechos fundamentales en el ordenamiento español se contiene en el art. 53 CE, y se articula en torno a «*tres niveles generales de protección de los derechos»* [39].

No parece necesario un estudio en profundidad de la protección de cada derecho fundamental, y por ello es preferible centrar este apartado en la tutela que se brinda a los derechos del art. 18 CE, en tanto que son éstos los que se pretenden proteger con la regulación de las medidas de investigación electrónica previstas en los arts. 588 sexies y 588 septies de la LECrim, en sus distintos apartados.

Los datos que se pueden albergar dentro de un dispositivo electrónico pueden ser tan heterogéneos, que pueden verse afectados derechos como el secreto de las comunicaciones, la intimidad personal y familiar, la propia imagen, así como algunos otros ya mencionados como la autodeterminación informativa o el entorno digital. De todos los derechos contenidos en el art. 18 CE sólo el relativo a la inviolabilidad del domicilio no está específicamente protegido en ninguna de las dos diligencias que se estudian en este trabajo, ya que cuenta con la legislación expresamente dedicada a regular la diligencia de entrada y registro en domicilio.

El Título VIII del libro II de la LECrim se denomina, tras la reforma operada por parte de la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, "*De las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la constitución*". Con esta denominación se despeja cualquier duda sobre qué derechos son los

[39] Cfr. TORRES DEL MORAL. Op. Cit. Pág. 595 y 596. El autor realiza una exposición y sistematización tradicional de la protección constitucional.

afectados por las diligencias que se exponen en su articulado, lo que justifica su análisis desde la óptica de su protección constitucional[40].

Cada uno de los capítulos del Título VIII LECrim, regula un modo de limitar los derechos del art. 18 CE. El Capítulo I regula la entrada y registro en lugar cerrado, el Capítulo II se refiere al registro de documentos, el Capítulo III a la apertura de la correspondencia, etc. El derecho al secreto de las comunicaciones, y su limitación mediante las intervenciones telefónicas o telemáticas y los que se refieren mas propiamente a la investigación electrónica se encuentran regulados en otros capítulos. Por lo tanto, una característica de la nueva regulación es que cada derecho fundamental de los contenidos en el art. 18 CE, cuenta con su propia diligencia de investigación limitadora.

En cambio, y a diferencia de las anteriores, las diligencias de investigación de los Capítulos VIII y IX de la LECrim resultan un tanto diferentes. La distinción reside en el número de hipotéticos derechos del art 18 CE que se pueden ver afectados, que en el caso de las diligencias de estos dos capítulos puede ser de un contenido muy diferente. Así mientras que, en las demás diligencias, suele ser un solo derecho el que se afecta, en el caso de estos dos capítulos se puede afectar a más de uno.

En todo caso, los derechos del art. 18 que se afectan serán los estrictamente relacionados con la intimidad, la imagen y a lo sumo el secreto de las comunicaciones, pese a alguna alusión referente al lugar en que sean encontrados los dispositivos.

En suma, puede decirse que la primera forma de protección jurídica de los derechos del art. 18 CE se conforma mediante el establecimiento de una regulación propia que configure el modo en que cada uno de estos derechos puede ser limitado. El texto legal actual cumple también con la garantía exigida por el art. 53 CE que exige que las normas que limiten alguno de estos derechos, sean leyes orgánicas.

El segundo modo de articular la protección jurídica de estos derechos es atribuir su limitación a la figura del Juez de Instrucción, encargado de su protección durante la investigación criminal. El Juez velará porque la limitación del concreto derecho constitucional del art. 18 CE se realice del modo más escrupuloso y excepcional posible, anteponiendo el derecho afectado a otros valores, circunstancias y derechos de mayor relevancia que los personales del investigado. Incluso aunque se abre la posibilidad de que la policía o el Ministerio Fiscal actúen limitando estos derechos, bajo circunstancias excepcionales, es el Juez Instructor el que debe confirmar esas actuaciones. Esta

[40] Hay más derechos constitucionales afectados e imbricados en el seno del proceso penal. En el caso de la fase de instrucción, que es en la fase en la que suele desplegar su contenido estas diligencias, alguno de los derechos constitucionales que hay que salvaguardar son, a título de ejemplo, el derecho de defensa y de acceso al contenido de las actuaciones. Sobre dicha facultad de acceso puede consultarse la Circular de la Fiscalía General de Estado 3/2018, de 1 de junio, sobre el derecho de información de los investigados en los procesos penales (Págs. 30 y siguientes)

regulación culmina las facultades del Juez para que se salvaguarden el conjunto de derechos fundamentales del investigado, no sólo los del art. 18 CE, que específicamente se analizan ahora, sino todos los demás que se imbrican en el proceso penal: el derecho de tutela judicial efectiva y sus derivados: defensa, última palabra, etc.

En tercer lugar, además de la regulación específica de cada modo de limitar el derecho del art. 18 CE y la atribución de ésta a los jueces, hay más modos de protección de los derechos del art. 18 CE. Se trata de los relacionados específicamente en la Constitución, especialmente el recurso de amparo (arts. 161.1b), y el art. 162, en relación con el art. 53.2 CE) regulado en una Ley Orgánica específica[41]. No se trata del único modo de protección de derechos fundamentales, ya que existen otros que afectan a otros derechos, como, por ejemplo, el habeas *corpus*[42], etc.

La protección de los derechos fundamentales también es una constante que se recoge en la normativa internacional, mucha de ella, ratificada por España. Entre estas normas destaca el Convenio europeo para la protección de los derechos humanos y de las libertades fundamentales y la protección que le brinda el Tribunal Europeo de Derechos Humanos. Se trata de una norma que es parte integrante del derecho comunitario[43] junto a los tratados fundacionales de la UE, los reglamentos y directivas, las normas esenciales de rango constitucional de los países miembros, etc. La defensa de los derechos que se citan en estas últimas normas citadas le corresponde al Tribunal de Justicia Europeo, que se encarga de su interpretación mediante los pareceres jurisprudenciales que dicta.

---

[41] Se trata de la Ley Orgánica 2/1979, de 3 de octubre, del Tribunal Constitucional. Título III, Capitulo primero, Artículos 41 y siguientes. Sobre su definición se puede consultar, Cfr. PEREZ TREMPS, Pablo. *El recurso de amparo*. Tirant lo Blanch. Valencia. 2015. Pág. 16 y 17.

[42] Se regula en la Ley Orgánica 6/1984, de 24 de mayo, reguladora del procedimiento de habeas corpus. Como ejemplo ilustrativo de la jurisprudencia constitucional sobre el mismo cabe citar, la STC 21/2018, de 5 de marzo de 2018. Ponente: Don Cándido Conde-Pumpido Tourón. La sentencia, establece por vez primera la doctrina del TC sobre el derecho a la libertad personal relacionado con el derecho a conocer los motivos de la detención, así como el derecho a la asistencia letrada. Además los pone en relación con el derecho a la libertad y su tutela por el proceso de habeas corpus. La sentencia realiza, además de lo anterior, un excelente resumen de distintas situaciones en las que se interpone el recurso de amparo. En el caso se recurría tanto la decisión de detención, como la posterior del Juez instructor en la que se denegaba la admisión a tramite del proceso de habeas corpus, lo que se conoce como *«recurso de amparo mixto»,* y en el mismo sentido se recuerda la cuestión del plazo de interposición del recurso cuando la decisión impugnada por atentatoria contra los derechos fundamentales provenga o bien de la autoridad gubernativa o lo haga de un Juez, siendo el segundo de los casos sometido a un plazo más breve que el primero. De hecho en el caso examinado, la decisión adoptada por el Juez no es examinada al considerar que el recurso se interpuso fuera de plazo, y por ello el examen del TC se centra en los derechos del detenido y en la información que debe recibir por ello tras las reformas operadas por la LO 13/2015, de 5 de octubre que traspone a nuestro derecho la Directiva 2010/64/UE, de 20 de octubre, relativa al derecho a interpretación y a traducción en los procesos penales, y la Ley Orgánica 5/2015, de 27 de abril, por la que se modifican la Ley de Enjuiciamiento Criminal y la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, para transponer la Directiva 2010/64/UE, de 20 de octubre de 2010, relativa al derecho a interpretación y a traducción en los procesos penales y la Directiva 2012/13/UE, de 22 de mayo de 2012, relativa al derecho a la información en los procesos penales. El TC acaba concluyendo con que el habeas corpus resulta un proceso apto para conocer de forma preferente si la detención es realizada de forma legal, pero incluye también en su objeto si la misma se ha realizado respetando el derecho a ser informado de las causas que la motivaron así como si se entregó la información en forma de atestado si fue solicitado.

[43] Vid. TORRES DEL MORAL. Op. Cit. Pág. 640.

Los derechos del art. 18 CE, además de la protección penal y procesal citada, cuentan con la protección ofrecida por la jurisdicción civil, que no es extrapolable a los demás derechos fundamentales. La LO 1/1982 de 5 de mayo del derecho al honor a la intimidad y a la propia imagen y sus aspectos derivados[44], es la que contiene esta protección. La doctrina matiza que no existe la misma modalidad de protección por vía de amparo para estos derechos en el ámbito del proceso penal, como lo sería para el derecho a la libertad el proceso de habeas corpus de la LO 6/1984, de 24 de mayo, por mandato expreso del art. 17.4 de la CE para el derecho a la libertad, cuya tutela permite acudir al amparo directo[45], lo que no existe para los derechos del art. 18 CE.

Seguidamente se procederá a delimitar cada uno de los derechos contenidos en el art. 18 CE, así como a analizar la protección que el ordenamiento jurídico brinda a cada uno de ellos.

1.1.3. El derecho al honor, a la intimidad y a la propia imagen: contenido y alcance.

En el apartado anterior se ha afirmado que la reforma procesal se dedica a regular el modo de limitar los derechos que se contienen en el art. 18 CE. Por consiguiente, parece adecuado realizar una exposición breve sobre el contenido de estos derechos del art. 18 CE de manera específica, en tanto que son los que pueden resultar comprometidos por la adopción de alguna de las diligencias de los Capítulo VIII y IX del Titulo VIII LECrim. Además resulta adecuado hacerlo dado el distinto contenido y alcance de cada derecho y la posible afectación conjunta de varios de estos derechos durante la práctica de cualquiera de estas diligencias.

El art. 18.1 CE no contiene uno, sino tres derechos distintos entre sí, con sus propias características, matices y alcances. Como derechos constitucionales que son, cada uno cuenta con su propia protección individual y concreta, reconocida a través de la jurisprudencia constitucional desarrollada mediante resoluciones dictadas tras el ejercicio del recurso de amparo[46]. Realizaré la

[44] Ibídem. Pág. 640.
[45] Vid. GIMENO SENDRA, Vicente. «Tutela procesal de los derechos fundamentales», en (GIMENO SENDRA et. al). Op. Cit. Pág. 673.
[46] En la STC 14/2003, de 30 de enero. Ponente: Don Vicente Conde Martín de Hijas, se pone de manifiesto un asunto en el que se fotografiaba a un policía deteniendo a una persona, se indicaba por el TC que es *«doctrina de este Tribunal, según la cual los derechos al honor, a la intimidad personal y a la propia imagen, reconocidos en el art. 18.1 CE, a pesar de su estrecha relación en tanto que derechos de la personalidad, derivados de la dignidad humana y dirigidos a la protección del patrimonio moral de las personas, tienen, no obstante, un contenido propio y específico. Se trata, dicho con otras palabras, de derechos autónomos, de modo que, al tener cada uno de ellos su propia sustantividad, la apreciación de la vulneración de uno no conlleva necesariamente la vulneración de los demás (SSTC 81/2001, de 26 de marzo, FJ2; 156/2001, de 2 de julio, FJ 3). Como hemos declarado en la última de las Sentencias citadas, el carácter autónomo de los derechos del art. 18.1 CE supone que ninguno de ellos tiene respecto de los demás la consideración de derecho genérico que pueda subsumirse en los otros dos derechos fundamentales que prevé este precepto constitucional, pues la especificidad de cada uno de estos derechos impide considerar subsumido en alguno de ellos las*

exposición de cada derecho resaltando no sólo su contenido, sino también la concreta protección que recibe desde el ámbito de la jurisdicción penal.

La esencia de los derechos del art. 18.1 CE se resumen en una idea clave, que es la de *«ser dejado en paz»* [47]. Es esta una expresión tan descriptiva como flexible, que permite aplicarla, con los debidos matices, a cada derecho del art. 18.1 CE. Esa simple definición resume la esencia a la que se ha aludido al inicio del párrafo y permite considerar esos derechos diferentes entre sí como distintas manifestaciones de un mismo aspecto.

El aspecto al que se refieren siempre estos derechos es al de la necesaria protección de un espacio abstracto, de carácter exclusivo e íntimo, excluyente y personal, de titularidad individual, preservado de cualquier clase de conocimiento externo atribuido a terceros. Los diferentes derechos que contiene dicho espacio abarcan y protegen la parcela más íntima de la propia vida. Esa parcela se aparta de toda intervención ajena, y de cualquier intromisión por los poderes públicos. En el caso de la intervención del Estado se puede matizar según el contenido concreto del derecho afectado. La parcela de intimidad personal puede ofrecer matices diferentes, y cada uno de estos matices son los que, separadamente constituyen cada uno de los derechos descritos en el texto.

El contenido de los derechos a la intimidad, al honor y a la propia imagen, parten del reconocimiento al individuo de un espacio propio, personal e individual y separado completamente de terceros. En este espacio el individuo se desarrolla y comporta libremente. Es un ámbito de la propia existencia apartado y vedado a cualquier clase de intromisión ajena; es *«la reserva que decide hacer la persona respecto de cierta información que considera que tiene que estar apartada de la vida del resto»*[48].

La amplitud de este concepto de reserva admite variadísimos matices, que son objeto de múltiples conflictos ocasionados por la imposición de cualquier tipo de limitación, intromisión o injerencia. Los ejemplos de estas injerencias son muy extensos y van desde la defensa del propio cuerpo

---

vulneraciones de los otros derechos que puedan ocasionarse a través de una imagen que muestre, además de los rasgos físicos que permiten la identificación de la persona, aspectos de su vida privada, partes intimas de su cuerpo o que se la represente en una situación que pueda hacer desmerecer su buen nombre o su propia estima. En tales supuestos la apreciación de la vulneración del derecho a la imagen no impedirá, en su caso, la apreciación de la vulneración de las eventuales lesiones del derecho a la intimidad o al honor que a través de la imagen se hayan podido causar, pues, desde la perspectiva constitucional, el desvalor de la acción no es el mismo cuando los hechos realizados sólo pueden considerarse lesivos del derecho a la imagen que cuando, además, a través de la imagen puede vulnerarse también el derecho al honor o a la intimidad, o ambos derechos conjuntamente (FJ 3; en el mismo sentido, SSTC 81/2001, de 26 de marzo, FJ 2; 83/2002, de 22 de abril, FJ 4)».

[47] Cfr. SERRANO MÁILLO. «Protección constitucional del honor, la intimidad y la propia imagen» en SÁNCHEZ GONZÁLEZ, Op. Cit. Pág. 205. A su vez la autora toma esta breve descripción del concepto de la doctrina anglosajona.

[48] Cfr. DONATO RAMÍREZ, Manuel Alejandro «Sobre el derecho a la intimidad. Breves reflexiones jurídicas», en LÓPEZ ORTEGA, Juan José (Dir,). *El derecho a la intimidad. Nuevos y viejos debates*. Dykinson, Madrid. 2017. Pág. 56.

humano ante las intervenciones de terceros (el pudor)[49], a la intimidad de los datos económicos[50], el que afecta a los reclusos internos en centros penitenciarios[51], pasando por el derecho a que se preserve el buen nombre profesional, familiar, los rasgos que identifican la propia imagen personal, etc.

Los tres derechos del art. 18.1 CE muestran, como segunda característica, una innegable dimensión civil, recogida en la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. La norma los define como derechos no absolutos, susceptibles de ser limitados cuando se den las circunstancias necesarias para ello[52]. Por lo tanto, lejos de ser derechos ilimitados, pueden ceder ante la colisión con otros derechos, tras una necesaria ponderación entre los distintos derechos en conflicto. Esta ausencia de carácter absoluto también se predica en el orden penal, que, según el texto de la ley, tiene preferencia a la civil.

Siguiendo el orden en que se relacionan en el art. 18.1 CE el primero es el derecho a la intimidad. El TC, en la sentencia que posteriormente dio lugar al pronunciamiento de la STEDH caso Rueda vs España (sentencia importante por cuanto dio lugar a la reforma legislativa actual), definió el derecho a la intimidad como la «*derivación de la dignidad de la persona (art. 10.1 CE), implica la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana (SSTC 207/1996, de 16 de diciembre, FJ 3; 186/2000, de 10 de julio, FJ 5; 196/2004, de 15 de noviembre, FJ 2; 206/2007, de 24 de septiembre, FJ 4; y 159/2009, de 29 de junio, FJ 3). De forma que «lo que el art. 18.1 garantiza es un derecho al secreto, a ser desconocido, a que los demás no sepan qué somos o lo que hacemos, vedando que terceros, sean particulares o poderes públicos, decidan cuales sean los lindes de nuestra vida privada, pudiendo cada persona reservarse un espacio resguardado de la curiosidad ajena, sea cual sea lo contenido en ese espacio» (SSTC 127/2003, de 30 de junio, FJ 7 y 89/2006, de 27 de marzo, FJ 5). Del precepto constitucional citado se deduce que el derecho a la intimidad confiere a la persona el poder jurídico de imponer a*

[49] STC 37/89, de 15 de febrero. Ponente: Don Francisco Rubio Llorente. Esta resolución dice sobre la intimidad que : «*Constitución garantiza la intimidad personal (art. 18.1), de la que forma parte la intimidad corporal, de principio inmune, en las relaciones jurídico-públicas que ahora importan, frente a toda indagación o pesquisa que sobre el cuerpo quisiera imponerse contra la voluntad de la persona, cuyo sentimiento de pudor queda así protegido por el ordenamiento, en tanto responda a estimaciones y criterios arraigados en la cultura de la comunidad*»

[50] Vid. BUENO GALLARDE, Esther. *La configuración constitucional del derecho a la intimidad. En particular el derecho a la intimidad de los obligados tributarios.* Centro de Estudios Políticos y Constitucionales. Madrid. 2009. Pág. 89 y siguientes. También puede consultarse como ejemplo de dicha manifestación del derecho a la intimidad en el ámbito económico y tributario el contenido de la STC 233/2005, de 26 de septiembre de 2005. Ponente: Don Guillermo Jiménez Sánchez.

[51] Puede consultarse, sobre aspectos interesantes del derecho a la intimidad, el contenido de la STC 186/2013, de 4 de diciembre. Ponente: Don Juan José González Rivas. La sentencia versa sobre los cacheos realizados a reclusos, para cuya práctica debían quedar desnudos y su implicación con el derecho aludido.

[52] Dice la Exposición de motivos de la norma que «*los derechos protegidos en la ley no pueden considerarse absolutamente ilimitados*».

terceros el deber de abstenerse de toda intromisión en la esfera íntima y la prohibición de hacer uso de lo así conocido (SSTC 196/2004, de 15 de noviembre, FJ 2; 206/2007, de 24 de septiembre, FJ 5; y 70/2009, de 23 de marzo, FJ 2)»[53]. La definición que se nos ofrece afianza la idea del espacio individual excluyente de cualquier injerencia externa.

El derecho a la intimidad también cuenta con tutela penal específica, que se encuentra en la tipificación como delitos de las conductas descritas en el Título X del Código Penal, concretamente en los arts. 197 y siguientes: delitos relativos al descubrimiento y revelación de secretos, el apoderamiento de documentos, la interceptación ilegal de comunicaciones, la divulgación no autorizada de imágenes y de grabaciones, el quebrantamiento de secretos profesionales, el allanamiento de morada, así como conductas que permiten acceder a los instrumentos necesarios para cometer estos delitos.

La doctrina considera dentro del ámbito procesal penal, que el derecho a la intimidad también se protege regulándose de modo detallado los supuestos en que procede limitarlo. Las diligencias de investigación que se analizan más adelante son el medio previsto por el legislador para tutelar y proteger el derecho a la intimidad, que queda preservado al regularse de qué forma y en qué casos se puede tener acceso a un dispositivo electrónico de uso personal, a su contenido y a los datos más diversos que dentro se pudieran encontrar y que pudieran afectar a este derecho. En relación a la actividad en internet, en la que se mezcla el derecho a la imagen o el honor, hay que recordar que «*las informaciones que una persona difunde en internet tienen carácter público»*[54], pero incluso esta actividad puede llegar a considerarse protegida por el art. 18 CE dentro del derecho al entorno virtual que se analiza más adelante.

La afectación del derecho a la intimidad durante la ejecución de alguna de las diligencias de investigación electrónica es evidente y puede resultar uno de los derechos más afectados, en tanto que los datos, que estén en el dispositivo incautado o registrado, se incluyen en un ámbito de protección primario subsumible dentro del derecho a la intimidad. Esto se debe a que se ha obtenido la información de un objeto de uso personal, y los datos que aloja son igualmente personales. El derecho al honor o el derecho a la propia imagen del art. 18.1 CE, pueden estar también afectados, pero para saberlo se requiere un examen más exhaustivo del contenido de cada uno de esos datos.

[53] STC 173/2011, de 14 de noviembre. Ponente: Don Eugenio Gay Montalvo.
[54] DELGADO MARTÍN, Joaquin. *La investigación tecnológica y la prueba digital en todas las jurisdicciones*. Wolter Kluwer. Madrid. 2016. Págs. 107. Ver, en especial las páginas 107 a 109, en las que el autor describe una manifestación propia del derecho a la intimidad en los dos aspectos señalados, esto es, la posibilidad de acceso al dispositivo utilizado, pero en especial se detiene en el acceso a los datos derivados de la actividad que el sujeto investigado desempeña en la red. El autor distingue en función de que se trate de una red abierta o de una red cerrada, lo que estima mucho más propio de delitos por ejemplo en los que se intercambian archivos electrónicos, etc.

No se puede desdeñar la posibilidad de una afectación simultánea y conjunta de estos tres derechos al mismo tiempo con un único acto de intromisión.

El siguiente derecho que se relaciona en el art. 18.1 CE es el derecho al honor, que es aquél que *«proscribe ser escarnecido o humillado ante sí mismo o ante los demás y garantiza, en términos positivos, la buena reputación de una persona, protegiéndola frente a expresiones o mensajes que la hagan desmerecer en la consideración ajena al ir en su descrédito o menosprecio o que sean tenidas en el concepto público por afrentosas»* [55].

En esencia, con el reconocimiento de este derecho, se protege el buen nombre, la reputación y la consideración de sus titulares, en un sentido amplio, que abarca también el crédito o prestigio profesional[56]. Se excluye a los demás sujetos de cualquier intromisión en el buen nombre, la fama, la consideración social y profesional de carácter individual.

Este derecho también cuenta con una tutela penal específica, circunscrita a la tipificación de las conductas descritas en los arts. 205 a 216 del Código Penal, donde se regulan los delitos de injurias y calumnias. Estos tipos penales consideran el honor como bien jurídico protegido. Desde el ámbito procesal penal, las diligencias de investigación tecnológica pueden afectar también el derecho al honor, aunque de forma más difusa y sutil de lo que puede suceder en el caso del derecho a la intimidad.

Es difícil que el honor pueda verse afectado por la mera investigación criminal, siendo además una obligación para los integrantes de las Fuerzas y Cuerpos de Seguridad del Estado, cuando tuvieran una noticia reveladora de comportamientos delictivos, investigarlos, lo que descarta cualquier actividad desviada que afectase a este derecho. Además, las últimas reformas procesales han sido muy sensibles con el derecho al honor de las personas detenidas, procurando la menor afectación posible al mismo[57].

Los particulares siempre pueden denunciar las concretas vulneraciones del derecho al honor que sufran, tanto por la vía civil, que más arriba se enunció, como por la vía penal, cuyos tipos también se han enumerado. Los tipos penales que protegen la intimidad y la imagen requieren expresamente

[55] STC 65/2015, de 3 de abril, Ponente: Don Francisco Pérez de los Cobos Orihuel. En esta sentencia, como en muchas otras donde se aborda este derecho, se está ante la contraposición con respecto al derecho a la libertad de expresión. En otras ocasiones, quizás las más sonadas, la contraposición del derecho al honor se entiende con respecto a otro derecho también esencial como lo es el de la libertad de información.

[56] STC 223/1992, de 14 de diciembre. Ponente: Don Rafael de Mendizábal Allende.

[57] Dispone el art. 520.1 LECrim tras la reforma de la Ley Orgánica 13/2015 que *«1. La detención y la prisión provisional deberán practicarse en la forma que menos perjudique al detenido o preso en su persona, reputación y patrimonio. Quienes acuerden la medida y los encargados de practicarla así como de los traslados ulteriores, velarán por los derechos constitucionales al honor, intimidad e imagen de aquéllos, con respeto al derecho fundamental a la libertad de información».*

la denuncia del titular del derecho al honor afectado[58], siendo denominados tradicionalmente como delitos privados, en los que sólo por esta vía cabe iniciar la acción penal.

En tercer lugar cabe hacer mención al derecho a la imagen. Según la jurisprudencia constitucional «*el derecho a la propia imagen pretende salvaguardar un ámbito propio y reservado, aunque no íntimo, frente a la acción y conocimiento de los demás; un ámbito necesario para poder decidir libremente el desarrollo de la propia personalidad y, en definitiva, un ámbito necesario según las pautas de nuestra cultura para mantener una calidad mínima de vida humana. Ese bien jurídico se salvaguarda reconociendo la facultad de evitar la difusión incondicionada de su aspecto físico, ya que constituye el primer elemento configurador de la esfera personal de todo individuo, en cuanto instrumento básico de identificación y proyección exterior y factor imprescindible para su reconocimiento como sujeto individual. En definitiva, lo que se pretende, en su dimensión constitucional, es que los individuos puedan decidir qué aspectos de su persona desean preservar de la difusión pública a fin de garantizar un ámbito privativo para el desarrollo de la propia personalidad ajeno a las injerencias externas»* [59].

Este derecho se refiere a la dimensión física del sujeto, a sus rasgos personales, y al derecho de evitar que cualquiera interfiera o se aproveche de la misma. Es un derecho que presenta un marcado carácter civil. Cuando se ve vulnerado, por ejemplo, mediante las publicaciones inconsentidas de fotografías en prensa o medios digitales, la ley permite al afectado ejercitar una acción tendente a ser resarcido por dicha publicación. El aspecto civil de este derecho es muy conocido para el gran público, por las recurrentes demandas civiles que en la tutela y salvaguarda de este derecho presentan las personas famosas. El derecho a la imagen de los menores de edad cuenta con cierta entidad propia, porque incluso queda fuera de la esfera de potestad de sus padres o tutores, lo que representa un modo especial de protección reforzada de este derecho en estos supuestos.

El derecho a la propia imagen también cuenta con una tutela penal específica. A diferencia de los demás tipos previstos para proteger otros derechos, éste se caracteriza por un aumento de las modalidades comisivas tipificadas. Los tipos penales que se han creado y que guardan relación con la aparición de la imagen de los menores son, por ejemplo, los delitos como la difusión de pornografía infantil[60], el acoso a menores empleando nuevas tecnologías[61], etc. Se trata de comportamientos que causan una gran alarma social, y guardan una evidente relación con la imagen

[58] Así lo exige expresamente el art. 215.1 CP salvo los casos en los que el afectado sea un funcionario, en cuyo caso este delito tradicionalmente considerado como privado pasa a ser un delito perseguible de oficio.
[59] STC 18/2015, de 16 de febrero. Ponente: Don Pedro José González-Trevijano Sánchez
[60] Ver arts. 186 y 189 del CP.
[61] Ver art. 183 ter, en especial el párrafo segundo, claramente dirigido a proteger las imágenes que pudieran obtenerse de menores de edad, si bien claramente ceñidas a actos de naturaleza sexual.

de las personas que se ven en los soportes que en cada caso consignen tales imágenes como consecuencia de la comisión de aquellos actos delictivos, en especial las víctimas. Los adultos también pueden ver vulnerado su derecho a la imagen, empleando la misma para finalidades ilícitas, como en el caso de la usurpación de identidad cometida a través del empleo de imágenes insertadas en documentos en los que éstas se encuentran[62].

El derecho a la imagen también puede verse afectado durante la práctica de alguna de las diligencias de investigación tecnológica. Por eso habrá que adoptar las medidas necesarias para evitar su lesión. La nueva regulación procesal permite al Juez que ordena la práctica de una diligencia de investigación electrónica, disponer los mecanismos y medios que estime en cada caso mas adecuado para que en los casos en que apareciesen imágenes, vídeos y demás formas de representación de la imagen que pudieran ser pertenecientes a la esfera privada del individuo investigado o de un tercero, solo accedan a las actuaciones penales los datos que pudieran afectar a estos derechos pero estrictamente relacionados con la causa, desechando los demás. Aunque el contenido de los autos que dispongan cualquiera de estas diligencias se tratarán más adelante, es conveniente tener en cuenta que dicho contenido es el resultado de una petición formulada previamente por los investigadores. Por ello es conveniente que éstos adviertan al instructor de la posibilidad de que se encuentren datos que pudieran afectar, al obtenerse, a este derecho, para que así el instructor pueda disponer los medios que estime más oportunos, y que eviten la filtración de datos que pudieran afectar al honor de la persona.

Cuando se analice el contenido específico de cada una de estas diligencias se verá como esta posibilidad, ha de ponerse de manifiesto especialmente en el inicio de la diligencia, más concretamente desde su petición. El momento inicial del dictado del auto en el que se acuerde la medida es donde habría de disponerse el modo en el que se practicará, y deben ser estas instrucciones las que determinen qué aspectos, especialmente por ser tocantes a tales derechos fundamentales, deben quedar apartados de la causa.

1.1.4. El derecho a la inviolabilidad del domicilio.

El art. 18.2 del texto constitucional consagra, de manera individualizada, el derecho a que los ciudadanos no vean violentada la intimidad atribuida a la morada propia, que se estima inviolable.

[62] El tipo penal descrito en el art. 401 del CP castiga con prisión de seis meses a tres años, a quien usurpa el estado civil de otro. Este precepto ha de ser puesto en relación con el art. Precedente, el 400 bis que penaliza el uso de determinados documentos por quien no está autorizado para ello. También cabe reseñar el contenido del art. 197 del CP

Por eso los accesos al domicilio habrán de ser siempre *«intromisiones, legalmente previstas, ocasionadas en virtud de una resolución judicial, flagrante delito o un estado de necesidad»* [63].

En relación con este derecho el ámbito de exclusión frente a terceros, del que se hablaba en el apartado anterior, se refiere a un ámbito material y físico, ceñido al lugar en el que se desarrolla efectivamente la vida privada y la vida familiar [64].

El Derecho limita al Estado la posibilidad de acceder a una vivienda que constituye morada, que solo puede verse excepcionada por dos vías: con el consentimiento al acceso efectuada por parte del titular del derecho (que deberá ser una exteriorización expresa e inequívoca) y, a falta de consentimiento, que éste se supla por la decisión judicial. En este segundo caso, la orden judicial que permita el acceso al domicilio valorará, ponderará y motivará la situación que requiere la entrada en dicho lugar cerrado.

El texto constitucional permite que la ausencia de consentimiento, e incluso la ausencia de resolución judicial, ceda ante una situación de emergencia que lo requiera. La situación de emergencia, como circunstancia legitimadora de la actuación limitadora del derecho, es un elemento al que se ha acudido también en la reforma del año 2015 para permitir la realización de alguna de las diligencias de investigación, como se verá. En algunos supuestos la ley permite que la Policía o el Ministerio Fiscal puedan llevar a cabo u ordenar que se ejecuten diligencias que expresamente admiten esta posibilidad, sin necesidad de autorización judicial previa. Estas medidas adoptadas en situaciones de emergencia o de necesidad, deben en todo caso pasar por el posterior control judicial que las confirme o las rechace. En todo caso se irán viendo en cada diligencia que se estudie.

El reconocimiento de este derecho exige partir de un concepto de vivienda o más bien de domicilio[65], porque es este espacio en el que se desarrolla el núcleo de la vida íntima, el objeto a proteger. Se trata de una categoría conceptual que ha ido ampliando su significado, aceptándose jurisprudencialmente que es vivienda todo aquel lugar en el que se desarrolla la vida privada: una caravana[66], una habitación de hotel, el camarote de un barco[67] o una tienda de acampada, siendo en la actualidad un concepto del que se sigue debatiendo[68].

---

[63] Cfr. CABEZUDO BAJO, María José. *La inviolabilidad del domicilio y el proceso penal.* Iustel. Madrid. 2004. Pág. 41.

[64] La STC 22/1984, de 17 de febrero. Ponente: Don Luis Díez-Picazo y Ponce de León, en su fundamento jurídico quinto desarrolla una de las primeras interpretaciones efectuadas por el TC sobre el derecho a la inviolabilidad del domicilio.

[65] Un estudio pormenorizado sobre el concepto de domicilio y sus características, podemos encontrarlo en CABEZUDO BAJO. Op. Cit. Págs. 117 y siguientes.

[66] STS 721/1996, de 18 de octubre. Ponente: Don Cándido Conde Pumpido Tourón.

[67] STS 151/2009, de 11 de febrero. Ponente: Don Adolfo Prego de Oliver y Tolivar.

[68] STS 972/2016, de 21 de diciembre. Ponente: Don Andrés Palomo del Arco. En la sentencia se recoge un estudio, muy interesante, del concepto de domicilio en distintas sentencias dictadas por el Tribunal Supremo. Pero, en especial, se

El derecho a la inviolabilidad del domicilio cuenta con una específica protección penal mediante los delitos tipificados en el art. 202 del CP. Por su parte, dentro del ámbito procesal penal, el derecho a la inviolabilidad del domicilio cuenta con una regulación específica que desarrolla el modo de llevar a cabo la entrada y registro en domicilio, en el contenido de los arts. 545 a 572 LECrim, dentro del Capítulo I del Título VIII. Se trata de uno de los derechos fundamentales del art. 18 CE, que como más arriba se aludió, cuenta con la regulación específica, concreta y exclusiva para efectuar su limitación. Por lo tanto, no parece que en el caso de las diligencias de investigación tecnológica de los Capítulos VIII y IX del Título VIII LECrim, exista regulación alguna sobre la afectación a este derecho.

En todo caso, el texto de los arts. 588 sexies a, y 588 sexies b, de la LECrim, reguladores de la diligencia de acceso a un dispositivo de almacenamiento masivo de información, distingue entre dos circunstancias, que el artefacto que se encuentra y que pudiera albergar dicha información sea encontrado dentro de un lugar susceptible de ser considerado como domicilio, o se haga fuera del mismo. Esta mención no tiene virtualidad reguladora en el derecho a la inviolabilidad domiciliaria.

La alusión que se hace en el precepto no pretende regular en ningún momento el acceso a un domicilio, porque no es su función, sino que lo que persigue es dejar tajantemente claro que una cosa es poder acceder al interior de un inmueble, contando para ello con la autorización judicial oportuna, y otra muy distinta es que, aprovechando que se accede al interior del mismo, quede subrepticiamente entendido que existe un derecho adicional, que abarca no ya la facultad de apoderarse del dispositivo encontrado, sino también cotejar el contenido de los instrumentos, efectos, aparatos y dispositivos encontrados en su interior. El precepto deslinda las dos cuestiones para negar, en ambas situaciones, el acceso al contenido de tales dispositivos dondequiera que sean ubicados.

El contenido del art. 588 sexies a. párrafo segundo LECrim lo prohíbe expresamente, y con ello quedan claramente deslindadas y delimitadas tanto las diligencias previstas dentro del Capítulo I, como además perfectamente perfilado el contenido de cada uno de los derechos del art. 18.1 y 2 de la CE. En el caso de la diligencia de registro remoto de equipos electrónicos, cuando la práctica de esta operación se lleve a cabo instalando un software espía, parece claro que puede resultar

---

hace eco del contenido de un acuerdo de Pleno de la Sala Segunda del Tribunal Supremo de 15 de diciembre de 2015 que aborda el concepto de garaje en edificios de propiedad horizontal, conforme al cual: *«los garajes comunes sitos en edificio de propiedad horizontal, tienen la consideración de dependencia de casa habitada, siempre que tengan las características siguientes: a) contigüidad, es decir, proximidad inmediata, absoluta, extrema o directa con la casa habitada; que obviamente puede ser tanto horizontal como vertical; b) cerramiento, lo que equivale a que la presunta dependencia esté cerrada, aunque no sea necesario que se halle techada ni siquiera murada; c) comunicabilidad interior o interna entre la casa habitada y la presunta dependencia; es decir, que medie, puerta, pasillo, escalera, ascensor o pasadizo internos que unan la dependencia donde se comete el robo con el resto del edificio como vía de utilizable acceso entre ambos. d) unidad física, aludiendo al cuerpo de la edificación».*

necesario solicitar una entrada y registro en domicilio para poder instalar dicho sistema de registro, pero en todo caso dicha entrada se realizará aplicando sus normas específicas [69].

1.1.5. El derecho al secreto de las comunicaciones: contenido y alcance.

El derecho constitucional al secreto de las comunicaciones ha sido uno de los más analizados. Es ingente el número de sentencias del Tribunal Supremo que versan sobre ello, y esto se debe a lo frecuente que resulta en la práctica emplear esta diligencia como medio de investigación. La evidente afectación a este derecho constitucional, que sólo permite la limitación judicial, ha hecho que su contenido haya sido enormemente tratado por la jurisprudencia constitucional[70].

La utilidad que presenta poder "pinchar" un teléfono como método para desvelar la participación de concretas personas en hechos delictivos es innegable. Su práctica permite poder conocer cómo y cuándo se perpetrará un delito. Hay delitos, como por ejemplo los de tráfico de estupefacientes, o los delitos de tráfico de personas que, en buena parte, se diseñan por los sujetos activos, empleando medios de comunicación.

Es un derecho, que por su ubicación en el texto constitucional, posee uno de los mayores grados de protección, y que la doctrina encuadra dentro del grupo de los tradicionalmente considerados como derechos civiles [71], es decir, el grupo de lo que hoy denominamos derechos fundamentales, más apegados a su concepción liberal: propiedad o intimidad, entre algún otro.

El contenido del art. 18.3 CE dispone que *«se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial»*. Se trata de un derecho que se integra en la *«libertad de comunicación»*[72], lo que implica la prohibición a los poderes públicos de inmiscuirse en los procesos de comunicación que se entablen por los ciudadanos, en cualesquiera de las formas en que ello es posible. Tiene su correspondencia, en el art. 8.1 del CEDH.

---

[69] Así lo pone de manifiesto la CFGE 5/2019, de 6 de marzo. Pág. 55-56.
[70] Desde casi los inicios del TC se pueden encontrar resoluciones en las que se da importancia a la necesidad de motivar la resolución que ordena la intervención de comunicaciones o sus prórrogas. Así sobre la primera cuestión se cita la STC 86/1995, de 6 de junio. Ponente: Don Vicente Gimeno Sendra, y sobre la segunda STC 49/1996 de 26 de marzo. Ponente: Don Manuel Pérez de Parga y Cabrera.
[71] Vid. TORRES DEL MORAL. «Fundamento, naturaleza y sujeto de los derechos», en (GIMENO SENDRA et. al), Op. Cit. Pág. 96.
[72] Cfr. ÁLVAREZ CONDE, Enrique y TUR AUSINA, Rosario. *Derecho Constitucional*. Tecnos. Madrid. 2016. sexta edición. Pág. 381.

El contenido del derecho protege el proceso de comunicación mismo, es decir, un proceso de intercambio de mensajes, pero también se extiende su contenido a los sujetos intervinientes en el proceso de comunicación[73], si bien la vulneración del derecho, cuando es el propio componente del proceso comunicativo, bien sea el emisor, bien el receptor, el que hace público o da a conocer el contenido de aquel proceso, no existe.

No puede descartarse de modo taxativo la afectación del derecho al secreto de las comunicaciones durante la ejecución de alguna de las diligencias de investigación objeto de estudio. En especial, bajo mi consideración, estimo que no puede descartarse la posible intervención durante la realización de la intervención de un ordenador de forma remota. Es hipotéticamente admisible que las comunicaciones que se realicen empleando el ordenador intervenido se vean afectadas[74]. El auto que acuerde la intervención remota debe ser el que limite, en lo posible, la toma de datos que no sean necesarios para la investigación, y se refieran a las comunicaciones directas, porque podría alcanzar datos que, sin saberlo, *«formen parte de un proceso de comunicación vigente…..o consumada»* [75]. En el caso de que se intervengan datos sobre un proceso de comunicación consumado el derecho afectado es el de la intimidad. Esta distinción ha sido una constante en la jurisprudencia, expresando la STS 489/2018, de 23 de octubre, que *«no es lo mismo un procedimiento de comunicación en marcha que un proceso de comunicación cerrado. Sólo el primero está indiscutiblemente vinculado al derecho al secreto de las comunicaciones. En el segundo caso se detectan profundas diferencias. Estaremos más bien en el campo de la intimidad, la privacidad o en su caso, la autodeterminación informativa»*[76]

La conclusión a la que puede llegarse es que no es imposible que el derecho al secreto de las comunicaciones se vea limitado de manera real y efectiva mediante las diligencias de acceso y registro de datos, ya que los ordenadores (y entiéndase por tal cualquier dispositivo similar a ellos), en la actualidad, son artefactos aptos para realizar una comunicación verbal o escrita. Permiten, incluso, que los comunicantes puedan observarse mutuamente, a modo de videoconferencia, pues aplicaciones tan extendidas como Skype, FaceTime, Hang Out, o similares, admiten realizar estas video llamadas que pueden verse intervenidas entre el cúmulo de operaciones generales que realice el ordenador del que se haya ordenado su acceso.

[73] STC 114/1984, de 29 de noviembre. Ponente: Don Luis Díez-Picazo y Ponce de León.
[74] La propia CFGE 5/2019, de 6 de marzo, estima que la diligencia de registro remoto de equipos está a medio camino entre el registro de dispositivos de almacenamiento y la intervención de comunicaciones.
[75] Vid. DELGADO MARTIN, Joaquín. *Investigación tecnológica y prueba digital …*. Op. Cit. Pág. 371. Se describe en el apartado dedicado a la legalidad de la medida de acceso a dispositivos electrónicos la posible afectación de todos los derechos que se encuentran dentro del art. 18 CE cuando se trata de datos que están dentro de un dispositivo electrónico.
[76] Fundamento jurídico cuarto con mención a la STS 528/2014.

Por el contrario, es menos probable la afectación al derecho al secreto de las comunicaciones en el caso de la práctica de la diligencia de registro de un dispositivo. El aparato intervenido tiene por único fin el de almacenar información, y aunque dicho artefacto pudiera realizar procesos de comunicación, la búsqueda se dirigiría a los datos ya creados y almacenados en su interior. Por eso es más dudoso e improbable, por no decir imposible, la obtención de datos de una comunicación en curso, y de afectar a estos procesos de comunicación, lo serían sobre comunicaciones ya finalizadas, como por ejemplo correos electrónicos ya abiertos, que afectarían al derecho a la intimidad.

En todo caso la enorme variedad de dispositivos que existen en la actualidad hace que no sea descartable esta posibilidad de afectar una comunicación en curso, siendo la resolución judicial que acuerde el acceso la que ha de prever la eventualidad de que se vean afectadas las comunicaciones. Ha de volverse nuevamente a la posibilidad que en la actualidad brinda la LECrim, para que sea el auto habilitante el que determine cualquier eventualidad que pudiera darse durante la práctica de una diligencia que afecta a los derechos del art. 18 CE. En este caso, y en relación al derecho al secreto de las comunicaciones, sería conveniente y oportuno que el mismo advirtiera de esa posibilidad según el tipo de aparato que se incautase, y determinar que la limitación al derecho al secreto de las comunicaciones exigiría resolución motivada independiente.

La anterior advertencia debe ser reforzada con la posibilidad de poder incurrir, caso de no ser debidamente apreciada la posibilidad, y se intervengan comunicaciones sin contar con decisión habilitante, con el contenido de lo que dispone el art. 197 del CP que tipifica la intervención no autorizada en las comunicaciones individuales, agravándose la pena cuando quien lo autoriza fuera un funcionario público[77].

1.1.6. El derecho al propio entorno virtual.

El contenido de los derechos del art. 18 CE ha sido analizado hasta aquí, desde una óptica individual, es decir, desde la del contenido esencial que presenta cada uno de ellos de forma separada. Pero dicha óptica ha de variarse en este apartado dedicado a examinar el contenido del nuevo derecho al entorno virtual. El estudio de este concreto derecho impone una dimensión o visión colectiva en la forma de entender todos los derechos del art. 18 CE. En palabras de la STS

[77] La STS 79/2012, de 9 de febrero. Ponente: Don Miguel Colmenero Menéndez de Luarca. la sentencia condena a un Magistrado de la Audiencia Nacional como autor de un delito de prevaricación derivado de la autorización de unas escuchas telefónicas realizadas entre un investigado y su letrado defensor.

489/2018, de 23 de octubre, el *«tratamiento jurídico puede ser más adecuado…si todos los datos….se contemplan de forma unitaria»*.

Se trata de un derecho que es el resultado de la evolución lógica de algunos de los problemas jurídicos que suscita el uso de aparatos e instrumentos electrónicos de almacenamiento y tratamiento de datos. Los ordenadores, y otros dispositivos digitales con funciones similares, son herramientas que permiten trabajar con ellos creando documentos, llevando la contabilidad de una empresa, hasta poder divertirse con su uso, viendo una película o una serie de televisión, pasando por conectarse internet y a redes sociales, recibir y enviar correos electrónicos o hasta guardar y editar fotografías y videos.

Cada una de las anteriores actividades enumeradas genera, desde un punto de vista técnico-informático, datos electrónicos que están expresados en un lenguaje informático. La acumulación de los datos generados por todas estas tareas, unidos a los demás datos que se generan por el propio acceso de estos dispositivos a internet o el empleo de redes sociales, permite a cualquier persona que reúna los conocimientos técnicos necesarios, hacer una lectura de los mismos y realizar un perfil completo del usuario del terminal informático. El estudio de este perfil permitirá conocer los gustos privados, las opiniones personales o las tendencias del usuario. En suma, se crea una detallada y precisa imagen virtual de este usuario.

El art. 18.4 CE dispone que *«la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos»*. La manifestación de esta expresión del texto constitucional se interpreta como el derecho a ser protegidos del uso que terceras personas pueden hacer de esos datos personales, pero no solo para tutelar los demás derechos del art. 18 como se dice expresamente, sino, como también dice el texto, para que se garantice el pleno ejercicio de los derechos en general. Por lo tanto, la protección de los datos personales entronca, a su vez, con la tutela del derecho a la intimidad y del honor del art. 18.1 CE, ya analizados [78], pero también con el pleno ejercicio y disfrute de los demás derechos del individuo.

[78] La STC 29/2013, de 11 de febrero. Ponente: Don Fernando Valdés Dal-Ré, realiza un interesante análisis del llamado derecho a la autodeterminación informativa, es decir, el derecho a que conozcamos qué datos se tienen de nuestra actividad. Se trata de un supuesto entroncado con el Derecho Laboral en el que un funcionario es sancionado por faltas de asistencia a su puesto de trabajo en una Universidad. Este centro público usó como prueba en el juicio unas grabaciones que acreditaban que solía llegar tarde a su trabajo. La problemática del uso de esos datos se analiza en los fundamentos cuarto y quinto el derecho afectado. Es interesante el resumen que se realiza en el fundamento sexto de la resolución que citando otros pareceres del mismo tribunal indica que: «*En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado … Pero ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin*». Por su parte la STS 489/201, DE 23 de octubre, pone en relación el derecho del art. 18.4 con aspectos como la geolocalización.

Esta concreta disposición constitucional está siendo objeto de aplicación práctica mediante el reconocimiento a los individuos de nuevos derechos que los protegen de los efectos del uso intensivo de la tecnología. La protección de datos que constituye la finalidad principal de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales[79], es una clara manifestación del avance en la protección de los derechos individuales en materia digital, porque establece los mecanismos generales de tutela de los datos personales y reconoce y recoge algunos de los derechos más demandados dentro del ámbito de la protección de datos y del uso de la tecnología de la información.

Esta última ley citada es deudora directa, a su vez, del Reglamento Europeo 2016/679, de 27 de abril de 2016, que deja sin efecto a la Directiva 95/46. Es un reglamento que pretende ampliar el alcance del art. 8.1 de la Carta de los Derechos Fundamentales de la Unión Europea [80] y del art. 16.1[81] del Tratado de Funcionamiento de la Unión Europea sobre la protección de datos de carácter personal de las personas físicas [82], y entró en vigor el pasado 25 de mayo de 2018 [83], obligando a los países miembros a la adaptación de la normativa interna, que en España fue objeto de una adaptación parcial [84], seguida posteriormente por la aprobación de la nueva Ley Orgánica mencionada.

En estas normas se recogen diversos derechos, todos ellos relacionados con la protección de datos, como el de rectificación, el derecho de acceso (arts. 13 y 14) y el de cancelación de datos que obren en poder de entidades públicas o privadas (art. 15), así como nuevos derechos como el de

[79] BOE 294 de 6 de diciembre de 2018. La norma deroga la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, así como por el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, que fueron las primeras normas españolas sobre este particular.

[80] El artículo 8 dispone bajo la rúbrica «*Protección de datos de carácter personal»* que*: «1.Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente».*

[81] El artículo 16 dispone: «*1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.2. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes. Las normas que se adopten en virtud del presente artículo se entenderán sin perjuicio de las normas específicas previstas en el artículo 39 del Tratado de la Unión Europea».*

[82] Ver los considerandos 1, 9, 10, 13, 24 por citar algunos ejemplos. Cabe destacar que queda excluido del ámbito de protección de la norma el derecho de proteger los datos a las personas fallecidas (considerando 27).

[83] Art. 51 del Reglamento.

[84] Se trata del Real Decreto Ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos. El Real Decreto ha sido convalidado mediante resolución de fecha 6 de septiembre de 2018, publicada en el Boletín Oficial del Estado de 15 de septiembre de 2018, nº 224.

portabilidad de los datos[85], el derecho de supresión (conocido coloquialmente como "derecho al olvido" que se recoge en los nuevos artículos 93 y 94 de la LO 3/2018)[86], que particularmente ha sido objeto de algunas sentencias importantes en el orden civil [87]. Esta nueva generación de derechos está pensada, según el legislador, para la llamada nueva era digital y comprende más derechos como el testamento digital, acceso a internet o una amalgama de derecho de naturaleza digital radicados en el ámbito laboral.

El Reglamento europeo persigue una exhaustiva protección de los datos de las personas físicas vivas - excluyendo los de las personas fallecidas-, siendo sensible a los datos de los menores de edad[88] y también los de las personas jurídicas.

El derecho a la protección de datos personales del art. 18.4 CE y el reconocimiento de nuevos derechos digitales no son el único medio para proteger a los ciudadanos de los datos que se recaban por parte de terceros, sino que el derecho al entorno digital es un medio más para favorecer dicha protección. En los apartados anteriores se ha visto que muchos de los datos que se encuentran electrónicamente en el interior de un dispositivo están directamente protegidos por uno u otro de los diferentes derechos constitucionales, pero ¿qué sucede cuando el número de datos que se encuentra dentro de un dispositivo es tan ingente que resulta imposible diferenciar qué dato está protegido por un derecho o por otro de los contenidos en el art. 18 CE? La respuesta que se de a la pregunta es muy importante, porque la ausencia de un modo adecuado de acceder a esos datos puede comportar el peligro de que su acceso a un concreto proceso penal se produzca vulnerando alguno de esos derechos constitucionales en juego.

---

[85] Art. 13.2 b), 14.2.c) y 20 del Reglamento. Cfr. APARICIO VAQUERO, Juan Pablo. «La protección de datos que viene: el nuevo Reglamento General europeo. The forthcoming data protection: the new European General Regulation». *Ars Iuris Salmanticensis Tribuna de Actualidad* Vol. 4, 27-34 Diciembre 2016, Pág. 30. El autor hace guardar alguna relación entre el derecho a la portabilidad y la transmisión de datos que ello comporta, al indicar que «*en ciertos casos, el titular puede solicitar al responsable la entrega de los datos que le facilitó y que lo haga en un formato estructurado, de uso común y lectura mecánica, para dárselos a otro responsable; puede solicitar, incluso, que tales datos se transmitan directamente entre ambos responsables (el antiguo y el nuevo), si es técnicamente posible*».

[86] Art. 17 del Reglamento.

[87] Sobre el derecho al olvido digital cabe enunciar varias resoluciones dictadas por la Sala Primera, de lo civil, del TS, y en las que ha resultado ponente siempre el Magistrado D. Rafael Sarazá Jimena, entre las que hay que destacar la STS 545/2015, de 15 de octubre, la STS 210/2016, de 5 de abril de 2016, la STS 426/2017, de 6 de julio y la STS 446/2017, de 13 de julio. A efectos meramente ilustrativos cabe decir que la jurisprudencia de la Sala Primera del TS sobre el particular hace responsables del tratamiento a las empresas multinacionales que tienen su domicilio social en el extranjero, pero cuentan con algún establecimiento abierto en España. En pocas palabras, el derecho al olvido digital no es más que la posibilidad del particular de solicitar a estas empresas que eliminen de sus buscadores cualquier resultado que los mismos arrojen empleando sus datos personales, fundamentalmente su nombre y apellidos. Con la nueva ley orgánica 3/2018, de 5 de diciembre, sobre protección de datos, se regula este derecho al olvido digital en los arts. 93 y 94.

[88] Así se desprende del contenido del considerando 1 del Reglamento 2016/679, puesto en relación con los considerandos 27 y 38. Con respecto a las personas jurídicas hay que acudir al contenido del considerando 14. Sobre la situación del tratamiento de datos personales de menores de edad ver el contenido del art. 8 del Reglamento que establece el necesario consentimiento del titular de la patria potestad.

En línea con la protección de los derechos fundamentales del art. 18 CE, y con la clara voluntad de otorgar una tutela integral a los diversos datos que componen el perfil digital de una persona, nace el llamado derecho al propio entorno virtual. Se trata de un derecho reconocido por vía jurisprudencial, porque su contenido no está reconocido ni en la Constitución, ni en la LOPDPGDD, ni en ninguna otra norma jurídica. Este derecho es la suma de toda una serie de derechos constitucionales superpuestos, y que con el contenido de esta doctrina son protegidos de modo conjunto, en una interpretación mucho más acorde y apropiada a la realidad social dominante en nuestros días. En el año 1978, no se podía imaginar el incuestionable avance tecnológico producido en nuestros días, lo que exige una necesaria adaptación del texto constitucional a las nuevas circunstancias sociales.

La base fáctica del derecho al propio entorno virtual o también llamado entorno digital, es la diseminación de datos que propicia el uso masivo de la tecnología, ya que *«todos aquellos instrumentos o aparatos susceptibles de almacenar información de manera digitalizada, acaban por crear un entorno virtual de la persona que se corresponde con una intimidad o confidencialidad»*[89]. De modo más profundo, el análisis y estudio sistemático de todos esos datos, admite la obtención de unos resultados muy concretos que se plasman en la recreación de un perfil de cada sujeto que permitiría realizar acciones predictivas, conocer sus tendencias sexuales, su ideología política, sus tendencias y preferencias de compra, sus contactos, sus gustos personales tanto positivos como negativos, etc. La amalgama de estos datos tan heterogéneos configura el llamado entorno digital [90]. Las enormes posibilidades que brindan estos datos dispersos, que resultan aptos para poder realizar con ellos perfiles de los ciudadanos, exige que la facultad del Estado para hacerse con esta clase de datos deba limitarse, para evitar que éste pueda disponer de un perfil de los ciudadanos, lo que resultaría contrario al respeto más básico a su intimidad.

El entorno virtual no es un contorno personal creado de forma consciente por el sujeto, sino que es el resultado de la recopilación de los datos generados como consecuencia del uso de los propios dispositivos electrónicos. Son las "migas de pan" abandonadas por el camino de quien, no es consciente del rastro que deja su paso por el mundo digital. Este rastro electrónico está conformado por datos que se ven afectados por diferentes derechos del art. 18 CE, aspecto este que ha sido

[89] Cfr. BONILLA CORREA, Jesús Ángel «Los avances tecnológicos y sus incidencias en la ejecución de la diligencia de registro en domicilio (1)». *Diario La Ley*, Nº 8522, 20 de Abril de 2015Pág. 3.
[90] Son sentencias que se ocupan de este derecho las STS 342/2013, de 17 de abril. Ponente: Don Manuel Marchena Gómez. y la STS 786/2015, de 4 de diciembre. Ponente: Don Manuel Marchena Gómez.

reseñado por la doctrina y la jurisprudencia[91] que muestra dudas sobre el tratamiento, que debe darse cuando debe llevarse a cabo una limitación sobre los mismos.

El desarrollo teórico de esta doctrina jurisprudencial impone un tratamiento conjunto y unitario cuando hay que limitar varios de los distintos derechos fundamentales del art. 18 CE. De esta forma, a pesar de que el tenor literal del texto constitucional no exige ni el mismo proceso ni los mismos requisitos a unos derechos que a otros, todos quedan tratados de la misma forma a la hora de limitarse. La aplicación de esta nueva doctrina jurisprudencial implica que ya no es necesario deslindar el contenido del derecho a la intimidad por una parte, del relativo al derecho al secreto de las comunicaciones, por otro, sino que todos los derechos del art. 18 CE implicados en el asunto en cuestión son valorados, a la hora de limitarse, de manera conjunta y se limitan aplicando el más alto grado de protección. La doctrina lo considera como un *«derecho de última generación nacido en el seno del nuevo universo de la revolución digital»*[92].

La Fiscalía General del Estado también reconoce el contenido de esta doctrina, y del derecho que la misma genera, y la reseña al estudiar los derechos que se ven afectados por las diligencias de

[91] Vid. MARCHENA GÓMEZ, Manuel; GONZÁLEZ CUÉLLAR SERRANO, Nicolás, *La reforma de la Ley de Enjuiciamiento Criminal en 2015*. Ediciones jurídicas Castillo de Luna. Madrid. 2015. Pág. 371. El autor cita expresamente distintas sentencias del TC, en concreto la 114/1984, de 29 de noviembre, Ponente: Don Luis Diez Picazo y Ponce de León, la 70/2002, de 3 de abril, Ponente: Don Fernando Garrido Falla la 120/2002, de 20 de mayo Ponente: Don Fernando Garrido Falla, la 123/2002, de 20 de mayo. Ponente: Doña María Emilia Casas Bahamonde y la 230/2007, de 5 de noviembre, ponente: Doña María Emilia Casas Bahamonde. En todas ellas se da como constante la tensión entre distintos derechos contenidos en el art. 18 CE; en la primera de las citadas, la 114/1984, de 29 de noviembre, se alude al proceso comunicativo y al hecho de si alguno de los intervinientes en dicho proceso guarda el deber de secreto de comunicaciones y no pueden hacer publica una conversación en la que intervinieron. Se concluye diciendo que no se ve afectado este derecho sino el derecho a la intimidad, al estar a lo sumo ante un deber de reserva. La segunda resolución citada, la 70/2002, de 3 de abril, ya se plantea el papel de las nuevas tecnologías y se cuestiona nuevamente el alcance de los arts. 18.1 y 18.3 ante el acceso a una carta ya abierta consignada dentro de una agenda que intervinieron los agentes. Se habla del proceso de comunicación como elemento esencial del derecho del art. 18.3 y se concluye que lo que se protege es el proceso mismo, y se entiende que cuando se ha concluido, como lo es en el caso de una carta ya abierta, lo afectado es la intimidad. La sentencia 230/2007, de 5 de noviembre, se refiere también a la importancia de las nuevas tecnologías, pero esta vez se alude al conflicto entre el derecho a la inviolabilidad del domicilio y a un aspecto derivado del art. 18.3; en concreto a si forma parte del mismo el conjunto de datos asociados a la comunicación tales como los que recaban las compañías telefónicas para poder tarifar. Se entendió que el proceso comunicativo se extiende a los datos que pudieran determinar quiénes son los integrantes de dicho acto, y por ello se requiere resolución judicial. Por último, en esta última sentencia, se entiende que el derecho al secreto de las comunicaciones también se extiende, siguiendo con la idea sentada en la sentencia anterior, a los listados de llamadas entrantes y salientes que obran grabadas en el teléfono móvil del sujeto investigado, y que para acceder a ellas hace falta resolución judicial. También cabe citar las sentencias 342/2013 y 587/2014, estas dos últimas del Tribunal Supremo. Lo que reseñan los autores es el hecho de que no resulta nuevo el cuestionamiento de la posible superposición de derechos constitucionales cuando hablamos de la información contenida en un artefacto electrónico, y con estas sentencias se hace eco de este extremo así como del parecer de estos tribunales sobre el particular. Además de las que cita el autor cabe destacar también, por recientes la STS 204/2016, de 10 de marzo. Ponente: Don Cándido Conde Pumpido Tourón y la STS 287/2017, de 19 de abril. Ponente: Don Manuel Marchena Gómez.

[92] Cfr. RODRÍGUEZ LAINZ, José Luis, «Sobre la pretendida dimensión formal del derecho al entorno digital. (A propósito de la STS, Sala 2ª, 489/2018, de 23 de octubre)». SEPIN, Febrero 2019. Referencia: SP/DOCT/81702. Pág. 4.

investigación electrónica, destacando como lo más característico del nuevo derecho, su efectiva aplicación práctica que consigue un *«tratamiento unitario de los derechos comprometidos»*[93].

Por consiguiente, estamos ante un derecho fundamental, de carácter general, reconocido por la jurisprudencia, y que otorga protección a los datos que se generan como consecuencia del empleo de dispositivos electrónicos, con independencia del derecho constitucional que individualmente proteja a cada dato de modo individual. Desde una vertiente estrictamente procesal, el derecho al entorno digital se traduce en un tratamiento homogéneo en la forma de limitar todos los derechos que conforman dicho entorno. Además, permite superar los problemas derivados de la divergencia en las previsiones constitucionales en cuanto a los modos de efectuar dichas limitaciones a su contenido

El tratamiento homogéneo y unitario, destacado por doctrina y jurisprudencia conlleva, siempre que esta doctrina sea de aplicación, que sea siempre un Juez el encargado de autorizar la medida que limite los derechos del art. 18, pese a que el texto constitucional no lo exigiera expresamente, sin que importe la preponderancia de un derecho sobre otro. El supuesto de hecho al que le es aplicable el derecho al entorno digital se circunscribe a dos circunstancias: a los casos en que los diferentes derechos del art. 18 CE se superponen y se entremezclan entre sí, y que estemos ante una investigación en la que el objeto de análisis es un dispositivo electrónico donde se encuentran datos que pueden afectar al contenido de uno o varios de los derechos del art. 18 CE.

En consecuencia, puede decirse que el derecho reconocido por la doctrina y la jurisprudencia sobre el entorno digital no desconoce ni olvida la jurisprudencia general sobre cada derecho fundamental del art. 18 CE, sino que la completa y coexiste con ella. La conclusión que puede obtenerse es que no se aplicará este nuevo derecho cuando cada derecho del art. 18 CE pueda ser analizado por separado, o bien estemos ante situaciones en las que sólo uno de ellos es el que se va a limitar, o bien tampoco cuando pese a que se vaya a limitar más de uno de estos derechos, no nos encontramos ante un dispositivo electrónico. En estos casos no siempre se requerirá la autorización judicial para limitar el derecho, sino que puede hacerse por los agentes investigadores, como se pone de manifiesto en situaciones como los cacheos superficiales o situaciones parecidas[94]. Por el contrario, cuando sean varios los derechos del art. 18 CE que pueden afectarse por una medida de investigación, y cuando la misma deba ser realizada mediante el estudio y análisis de dispositivos

[93] Circular de la Fiscalía General del Estado 5/2019, de 6 de marzo. Pág. 4.

[94] Así lo recuerda la ya mencionada STS de 28 de octubre de 2018, que realiza un recorrido por el modo de limitar los diferentes derechos del art. 18 CE, y aclara que si bien cada uno de ellos por separado pueden ser limitados sin autorización judicial cuando llegue el caso necesario, a excepción del que expresamente requiera dicha autorización, en los casos en que se desarrolla el derecho al entorno virtual (supuestos de investigación sobre dispositivos electrónicos en los que se superponen estos derechos), el legislador ha optado por un tratamiento homogéneo y unitario en la limitación de su contenido atribuido al Juez.

electrónicos, ha de ser aplicado el nuevo derecho al entorno digital.

Este derecho al propio entorno virtual ha sido reconocido legislativamente en el modo en que se disponen las distintas diligencias de investigación electrónica contenidas en la LECrim, otorgando a todo el título una verdadera unicidad comprensiva[95]. Un rasgo que destaca en el tratamiento jurídico de las medidas de investigación electrónica que contempla la ley es el método común que, en algunos aspectos, reciben las diligencias que se realizan mediante sistemas electrónicos y que, con independencia de su concreto contenido, deben ajustarse a los apartados generales de los arts. 588 bis a y siguientes LECrim. De entre todos estos apartados lo más destacable es la necesidad de autorización judicial.

El reconocimiento de este nuevo derecho por una parte, así como el tratamiento jurídico, que desde la reforma de la LECrim, reciben las diligencias de investigación electrónica, contribuyen a proteger el perfil digital de los ciudadanos, a reforzar los derechos del art. 18 CE en la medida en que no se atiende al contenido particular de cada uno, sino a la suma de todos ellos, y además ayuda a despejar cualquier duda de legalidad derivada de la limitación de alguno de estos derechos que podía plantearse al hacerse por separado. Las respuestas a esas dudas de legalidad se solventan desde el punto de vista legislativo con la necesaria intervención judicial para realizar cualquier limitación, cuando ésta sea necesaria en el ámbito de investigación criminal circunscrito a la investigación electrónica, con independencia, de que cada derecho individualmente considerado, la exija o no.

La doctrina que fundamenta este derecho no es nueva, existiendo precedentes jurisprudenciales que abogaban por la necesidad de tener en cuenta la pluralidad de derechos afectados cuando se trata de acceder a los diferentes datos alojados en un ordenador [96]. En estas resoluciones se alertaba del uso cada vez más habitual de la informática, y que obligaba a que se fijase alguna protección para los datos que este uso generase[97].

---

[95] Todas las diligencias de investigación del Titulo VIII LECRIM son referidas a diferentes medidas en la que se ven implicados, de un modo u otro, alguno de los derechos del art. 18 CE. De un modo más concreto, las de los Capítulo V y siguientes son exclusivamente electrónicas El derecho al entorno digital, que confiere al Juez instructor, la facultad para valorar y analizar la necesidad de realizar o no dichas diligencias se plasma en todas y cada una de las diligencias electrónicas descritas dentro del Título, pues todas estas sin excepción, son aprobadas por un Juez, tras un proceso de valoración, sin tener en cuenta el concreto derecho implicado. Sólo desde esta óptica puede comprenderse el título que se le ha dado al VIII, cuando sin distinción se refiere a «los derechos reconocidos en el artículo 18 de la Constitución».

[96] Sirve de ejemplo la STS 2324/1993, de 24 de junio de 1993, y la STS 2054/1993, de 10 de junio de 1993. En ambas resoluciones es Ponente D. Enrique Ruíz Vadillo. En las dos resoluciones comienza a advertirse el uso de los ordenadores como contenedores de numerosos datos e información susceptibles de ser preservados.

[97] STC 173/2011, de 7 de noviembre. Ponente: Don Eugenio Gay Montalvo. El tenor literal de la sentencia disponía: «*si no hay duda de que los datos personales relativos a una persona individualmente considerados, a que se ha hecho referencia anteriormente, están dentro del ámbito de la intimidad constitucionalmente protegido, menos aún pueda haberla de que el cúmulo de la información que se almacena por su titular en un ordenador personal, entre otros datos sobre su vida privada y profesional (en forma de documentos, carpetas, fotografías, vídeos, etc.) -por lo que sus*

El derecho al entorno virtual, como todos los del art. 18 CE, no es un derecho absoluto[98], sino que se puede limitar ante razones justificadas y debidamente ponderadas, siendo el contenido del art. 588 bis a LECrim el que determina los principios y aspectos que deben tenerse en cuenta a la hora de valorar la adopción de alguna diligencia en la que este derecho sea aplicable. Pero la limitación al derecho al entorno virtual también debe ser valorada caso a caso.

Sirva como ejemplo de la limitación al derecho al entorno virtual el supuesto de registro de un instrumento electrónico en el que se alberguen datos protegidos de más de una persona, como es el caso de un ordenador que usan todos los miembros de una misma familia o varios trabajadores de una empresa. La jurisprudencia ha encontrado en tales casos justificación para que la entidad digital individual se desdibuje, en la medida en que existe cierta admisión del beneficiado por el derecho cuando comparte los datos que configuran tal perfil con otras personas sin haber establecido sistemas que limiten dicho uso compartido[99].

En conclusión, puede decirse que el reconocimiento del derecho al entorno virtual presenta una serie de ventajas que pueden resumirse en los siguientes aspectos. En primer lugar, la creación de

---

funciones podrían equipararse a los de una agenda electrónica-, no sólo forma parte de este mismo ámbito, sino que además a través de su observación por los demás pueden descubrirse aspectos de la esfera más íntima del ser humano. Es evidente que cuando su titular navega por Internet, participa en foros de conversación o redes sociales, descarga archivos o documentos, realiza operaciones de comercio electrónico, forma parte de grupos de noticias, entre otras posibilidades, está revelando datos acerca de su personalidad, que pueden afectar al núcleo más profundo de su intimidad por referirse a ideologías, creencias religiosas, aficiones personales, información sobre la salud, orientaciones sexuales, etc. Quizás, estos datos que se reflejan en un ordenador personal puedan tacharse de irrelevantes o livianos si se consideran aisladamente, pero si se analizan en su conjunto, una vez convenientemente entremezclados, no cabe duda que configuran todos ellos un perfil altamente descriptivo de la personalidad de su titular, que es preciso proteger frente a la intromisión de terceros o de los poderes públicos, por cuanto atañen, en definitiva, a la misma peculiaridad o individualidad de la persona. A esto debe añadirse que el ordenador es un instrumento útil para la emisión o recepción de correos electrónicos, pudiendo quedar afectado en tal caso, no sólo el derecho al secreto de las comunicaciones del art. 18.3 CE (por cuanto es indudable que la utilización de este procedimiento supone un acto de comunicación), sino también el derecho a la intimidad personal (art. 18.1 CE), en la medida en que estos correos o email, escritos o ya leídos por su destinatario, quedan almacenados en la memoria del terminal informático utilizado. Por ello deviene necesario establecer una serie de garantías frente a los riesgos que existen para los derechos y libertades públicas, en particular la intimidad personal, a causa del uso indebido de la informática así como de las nuevas tecnologías de la información».

[98] Cfr. RODRÍGUEZ LAINZ, José Luis, «Sobre la pretendida dimensión formal…». Op. Cit. Pág. 4. El autor sostiene con cita en varias sentencias que se trata de un derecho que cede ante otros intereses.

[99] STS 287/2017, de 19 de abril. Ponente: Don Manuel Marchena Gómez. La sentencia establece que «*Es evidente que la utilización de un ordenador por todos o varios de los miembros de una familia introduce una doble singularidad que merece ser destacada. De una parte, porque, con carácter general, el desafío probatorio que incumbe a la acusación a la hora de probar la autoría de un hecho ligado al empleo de las nuevas tecnologías, exigirá siempre un esfuerzo argumental más depurado e intenso. Desde otra perspectiva, porque la reivindicación de una hipotética vulneración del derecho a la intimidad, en los supuestos de utilización compartida de un ordenador, no podrá prescindir de un hecho tan determinante como, por ejemplo, el uso común de una contraseña de acceso. Y es que, frente a lo que sucede respecto del contenido material de otros derechos, el derecho a la intimidad o, si se quiere, el espacio de exclusión que frente a otros protege el derecho al entorno virtual, es susceptible de ampliación o reducción por el propio titular. Quien incorpora fotografías o documentos digitales a un dispositivo de almacenamiento masivo compartido por varios es consciente de que la frontera que define los límites entre lo íntimo y lo susceptible de conocimiento por terceros, se difumina de forma inevitable. Desde luego, son imaginables usos compartidos de dispositivos de esa naturaleza en los que se impongan reglas de autolimitación que salvaguarden el espacio de intimidad de cada uno de los usuarios. Pero nada de esto se apunta en la resolución recurrida»*.

esta doctrina mejora el instrumento para el acceso a los datos personales que se encuentran en un dispositivo de almacenamiento masivo de información. Puesto que, se reserva la posibilidad de acceso a la orden dada por el juez instructor, y con ello se protege una posible afectación de cualquiera de los derechos del art. 18 CE[100], sustrayendo cualquier decisión sobre esos aspectos a la policía, o a cualquier otra autoridad gubernativa.

La segunda ventaja que ofrece es que reduce la necesidad de realizar un pormenorizado deslinde de cada derecho afectado por la medida limitadora, que hasta que se fue configurando esta doctrina resultaba necesario. La operación delimitadora se hacía imprescindible porque bajo la óptica individualizada de cada derecho, se podía efectuar un diverso enjuiciamiento sobre la correcta actuación realizada y sometida a examen. Esta delimitación consistía en valorar la necesidad de intervención judicial y examinar si la limitación se hizo de modo correcto o no. El reconocimiento del derecho permite reducir la operación valorativa, dirigiéndola hacia una operación evaluadora de las circunstancias que se predican en el caso y que favorecen la necesidad de practicar la medida limitadora, que en el caso de este derecho implica realizar la diligencia de investigación electrónica.

La tercera ventaja que aporta el reconocimiento del derecho desde una óptica procesal es que se despejan las dudas acerca del procedimiento de limitación. La plasmación práctica de este derecho

---

[100] Por su claridad a la hora de exponer un planteamiento del problema y la solución actual citaremos la SAP de Cádiz 335/2017 de 29 de diciembre. Ponente: Don Francisco Javier Gracia Sanz. Puede leerse en el fundamento segundo de la sentencia que «*El Juez a Quo hace referencia a la nueva regulación del registro de los dispositivos de almacenamiento masivo de información, donde se incluyen los ordenadores y móviles, introducida por la reforma de 2015.En efecto estos dispositivos se caracterizan por su multifuncionalidad (internet), gran capacidad de almacenamiento de información y potencialidad lesiva. Esa potencialidad lesiva en caso de injerencia indebida lo es de lesionar varios derechos fundamentales por poder contener:*
1.-Correos electrónicos: si aún no han sido abiertos por el destinatario constituyen comunicaciones telefónicas dinámicas igual que las de voz a través del teléfono protegidas por el secreto de las comunicaciones (art.18.3 CE) lo que requiere autorización judicial como garantía constitucional (STC 173/2011).
2-Fotos, videos o documentos con una potencial elevada carga de intimidad amparados por el art. 18.1 CE.
3.-Conversaciones de audio o voz estáticas incorporadas mediante aplicaciones de mensajería instantánea multipersonas (whatsapp) o en perfiles de redes sociales que también afecta a la intimidad amparada por el art. 18.1 CE .
4.-Datos personales amparados por el art. 18.4 CE.
5.*-Datos asociados al tráfico de las comunicaciones amparados por el derecho la intimidad (STC 206/2017 y 864/2015).*
Con anterioridad a la reforma de la Ley de Enjuiciamiento Criminal introducida por la LO 13/2015 el tratamiento era diferenciado en la legalidad constitucional de la injerencia si bien respecto de videos, fotografías o documentos no era necesaria la autorización judicial y resultando de aplicación, en general y con matizaciones, el principio de proporcionalidad, principio éste de innegable aplicación aquí ante la carácter ilícito penal de los hechos y la sospecha previa que el propietario albergaba. Tras la reforma se instaura con carácter general la regla de la necesidad de Autorización judicial. El legislador opta por reforzar las garantías y dar un tratamiento unitario a los datos contenidos en estos dispositivos ante el riesgo de eventuales excesos. Se acuña así el término "derecho a la protección del entorno virtual" como derecho constitucional de nueva generación. (STS Nº204/2016 de 10 de marzo). Y que ampara toda la información en formato electrónico que a través del uso de las nuevas tecnologías va generando el usuario (huella digital). Este reforzamiento supone, por ejemplo, la necesidad, entonces, de exteriorizar en un razonamiento diferenciado por el Juez que, además de la inviolabilidad del domicilio, es necesario hacerlo también de otros derechos mediante el registros de estos dispositivos, aunque sean hallados en un registro judicial, autorización que puede darse en el mismo auto de entrada o posteriormente".

se ciñe sólo al ámbito de investigación criminal relacionado con el estudio y análisis de cualquier clase de dispositivos electrónicos, y cuando esto sea necesario sólo será el Juez de instrucción el encargado de ordenar su práctica, permitiendo la ley determinados supuestos excepcionales de acceso por parte de los investigadores, pero que en todo caso también se ve sometido al principio de ratificación judicial inmediata.

La cuarta ventaja que aporta el reconocimiento de este nuevo derecho es que opta por el tratamiento más respetuoso posible, tanto para los derechos del propio investigado, como también para posibles terceros afectados por las medidas, porque somete a consideración judicial la oportunidad y necesidad de llevar a cabo la limitación de estos derechos, y obliga al Juez a que valore todos los aspectos que guardan relación con los derechos de terceras personas que pudieran verse implicadas como consecuencia de la adopción de la diligencia de investigación electrónica. Con ello se produce el ya aludido reforzamiento de los derechos individuales del art. 18 CE de cualquier persona y no sólo del investigado.

En quinto lugar, el reconocimiento de este derecho permite una mejor aplicación de determinados tipos penales relacionados, tanto con los derechos del art. 18 CE, como con los tipos que para la comisión delictiva emplean la electrónica y la informática. Es una doctrina que favorece una mejor interpretación de determinados bienes jurídicos protegidos, especialmente los que estén relacionados con varios de los derechos constitucionales que se han ido exponiendo y que se ven implicados en su contenido. La transmisión de este derecho a la norma legal se ha producido en este caso concreto, porque las nuevas diligencias de investigación electrónica permiten indagar íntegramente el entorno virtual sin atender al concreto derecho afectado por la medida.

En sexto y último lugar, es un derecho que permite aplicarse también a la información alojada en la nube y en redes virtuales. Lo relevante es siempre el contenido de los derechos que podrían verse afectados por el registro de esos datos, con independencia de que su ubicación sea física o virtual.

2.- Régimen jurídico de las diligencias de investigación relacionadas con el registro de datos electrónicos.

A.- Aspectos generales.

En este apartado del trabajo se va a analizar el marco teórico aplicable a las diligencias de investigación criminal de la LECrim que afectan o limitan a los derechos del art. 18 de la CE.

En primer lugar, y dado que las diligencias de investigación que contiene la reforma de la LECrim son muy distintas entre sí, se debe partir de los aspectos y presupuestos comunes a todas estas diligencias de investigación, con independencia del contenido concreto de cada una de ellas. Estos aspectos y presupuestos generales y comunes a todas las diligencias de investigación electrónica se regulan en el Capítulo IV del Título VIII de la LECrim.

Es un capítulo cuyo estudio permite conocer los criterios que son aplicables también a las diligencias de investigación reguladas en los arts. 588 sexies a) hasta 588 sexies c), y en los arts. 588 septies a) hasta el art. 588 septies c) de la LECrim; esto es, a la diligencia de acceso a los dispositivos susceptibles de albergar información de manera masiva, así como a la diligencia de acceso remoto a equipos informáticos.

Los conceptos teóricos y los requisitos generales que deben cumplirse para acordar la práctica de cualquier diligencia de investigación han de aplicarse también a la intervención de comunicaciones telefónicas y telemáticas, como para la grabación y captación de comunicaciones orales usando para ello medios electrónicos, en el uso de mecanismos técnicos de seguimiento, la localización y captación de la imagen, además de las otras dos ya enunciadas en el párrafo anterior.

1.- Clasificación de las diligencias de investigación. Propuestas de clasificación en función del derecho constitucional afectado o en función de los presupuestos y requisitos exigibles.

La reforma del texto del artículo 579 de la LECrim era una de las más esperadas modificaciones legislativas que se aguardaban en el derecho procesal penal español.

El texto de ese precepto, anterior a la reforma, concitaba una crítica generalizada, porque no permitía adoptar diligencias distintas a la simple intervención de la comunicación telefónica. Pero en cambio, en la práctica se usaba para recabar datos electrónicos, lo que ocasionaba con frecuencia la declaración de nulidad de la medida cuando no se ajustaba al canon jurisprudencial existente sobre la cuestión[101].

[101] SAN 25/2016, de 28 de septiembre. Ponente: Fermín Javier Echarri Casi. La sentencia hace un interesante estudio de las intervenciones de conversaciones ambientales. Así, en el Fundamento de Derecho Primero, apartado iv, pág., 25, hace alusión a la existencia de un auto habilitante que permitió llevar a cabo la diligencia consistente en la grabación de conversaciones entre dos personas al aire libre mediante el empleo de dispositivos especialmente colocados en los vehículos con dicha finalidad (por ello distinta a la diligencia de intervención telefónica) y que se amparó en el contenido del art. 579 LEcrim. Sobre este particular la Audiencia Nacional cita la sentencia del TC cuyo contenido citado en la sentencia se transcribe a continuación:
«*El artículo 579.2 LEcrim, como señala la STC 26/2006, de 30 de enero, adolece de vaguedad e indeterminación en aspectos esenciales, por lo que no satisface los requisitos necesarios exigidos por el artículo 18.3 CE para la*

Más concretamente, y sobre este precepto, la doctrina, en relación con el derecho al secreto de las comunicaciones *«considera que la regulación de la Ley de Enjuiciamiento Criminal no alcanza los requisitos mínimos para considerarla norma habilitante que dé cobertura legal a la intervención de las comunicaciones telefónicas»* [102]. Las carencias de contenido del art. 579 también fueron puestas de manifiesto, en muchas ocasiones, por el Tribunal Constitucional, el Tribunal Supremo y el Tribunal Europeo de Derechos Humanos[103].

La reclamada modificación legislativa se llevó a cabo mediante la promulgación de la LO 13/2015, de 5 de octubre, que incluyó un Capítulo III, denominado «*de la detención y apertura de la correspondencia escrita y telegráfica»*. Este capítulo se contiene, a su vez, dentro del Título VIII,

---

protección del derecho al secreto de las comunicaciones, interpretado, como establece el artículo 10.2 CE, de acuerdo con el artículo 8.1 y 2 CEDH ". En aquella, el Tribunal Constitucional analizaba una intervención de las comunicaciones entre dos sujetos en situación de detención. Y dice, "no es que la norma no resulte singularmente precisa al fin acordado (calidad de la ley); la objeción reside, antes que en ello, en que abierta e inequívocamente la norma invocada no regula una intervención secreta de las comunicaciones directas en dependencias policiales entre detenidos.....No estamos por lo tanto, ante un defecto por insuficiencia de la ley, ante un juicio sobre la calidad de la ley, sino que se debate el efecto asociado a una ausencia total y completa de ley. Y es que el artículo 579.2 LECrim se refiere de manera incontrovertible a intervenciones telefónicas, no a escuchas de otra naturaleza, ni particularmente a las que se desarrollan en calabozos policiales y entre personas sujetas a los poderes coercitivos del Estado por su detención, como las que aquí resultan controvertidas"; concluyendo que la posibilidad de suplir los defectos de la ley, no puede ser trasladada a un escenario de injerencia en el secreto de las comunicaciones en el que no exista previsión legal alguna».

En suma, ya estaba sentada la doctrina conforme a la cual fuera de las intervenciones telefónicas y de comunicaciones propiamente dichas, el artículo 579 de la LECrim no habilitaba para realizar intervenciones de cualquier otra naturaleza. Por su parte la STS 950/2013, de 5 de diciembre, Ponente: Don Julián Artemio Sánchez Melgar, en su fundamento de derecho primero, tras criticar el insuficiente contenido del art. 579, pone de manifiesto que la decisión judicial impugnada consistente en la adopción de la medida de intervención de comunicaciones, se ajusta a derecho porque a su vez cumple con la totalidad de los requisitos jurisprudencialmente exigibles para ello, inclusive el referente a la justificación de la medida por remisión al oficio policial.

[102] Cfr. LADRÓN TABUENCA, Pilar. «Las intervenciones telefónicas en el ordenamiento jurídico español: visión jurisprudencial». *La Ley pena*l nº 4. Abril de 2004. LA LEY 606/2004. Pág. 7.

[103] En palabras concretas de la STS 841/2016, de 8 de noviembre, en la que es ponente Don Juan Ramón Berdugo y Gómez De la Torre, y en la que al mismo tiempo se vista jurisprudencia del TC y del TEDH se pone de manifiesto lo siguiente: «*Sin embargo, la normativa legal reguladora de las intervenciones telefónicas es parca y carece de la calidad y precisión necesarias, por lo que debe complementarse por la doctrina jurisprudencial. Las insuficiencias de nuestro marco legal han sido puestas de manifiesto tanto por esta misma Sala, como por el TC (SSTC núm. 26/2006, de 30 de enero , 184/2003, de 23 de octubre , 49/1999, de 5 de abril) y el TEDH (SSTEDH de 18 de febrero de 2003, Prado Bugallo contra España y de 30 de julio de 1998 , Valenzuela Contreras contra España). La LECrim dedica a esta materia el art. 579 , en el Título VIII del Libro II, y las nuevas normas legales sectoriales no complementan adecuadamente sus insuficiencias, que requieren imperativamente y sin más demoras una regulación completamente renovada, en una nueva Ley procesal penal que supere la obsolescencia de nuestra legislación decimonónica»* .

Por citar alguna sentencia de fecha anterior a la reforma operada en la LECrim, cabe resaltar, la STS 855/2013 de 11 de noviembre. Ponente: Don Cándido Conde-Pumpido Tourón. En el fundamento jurídico sexto, página 9 de la sentencia se dice textualmente: «*La normativa legal reguladora de las intervenciones telefónicas es parca y carece de la calidad y precisión necesarias, por lo que debe complementarse por la doctrina jurisprudencial.*

Las insuficiencias de nuestro marco legal han sido puestas de manifiesto tanto por esta Sala, como por el TC (SSTC núm. 26/2006, de 30 de enero , 184/2003, de 23 de octubre , 49/1999, de 5 de abril) y el TEDH (SSTEDH de 18 de febrero de 2003, Prado Bugallo contra España y de 30 de julio de 1998 , Valenzuela Contreras contra España).

La LEcrim dedica a esta materia el art. 579 , en el Título VIII del Libro II, que es manifiestamente insuficiente, y las nuevas normas legales sectoriales no complementan adecuadamente dicha insuficiencia, que reclama imperativamente y sin más demoras una regulación completamente renovada, en una nueva Ley procesal penal que supere la obsolescencia de nuestra legislación decimonónica (STS 301/2013, de 18 de abril)».

denominado «*de las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución*».

En el nuevo texto de la ley se consignan de modo exhaustivo, pormenorizado, profuso e individualizado, todos los requisitos y presupuestos bajo los cuales pueden acordarse la práctica de cada una de las diligencias que pueden afectar a cada derecho de los contenidos en el art. 18 CE. Es destacable que la propia norma contenga los principios generales bajo los que cualquiera de las diligencias que contiene pueden ser adoptados, asumiendo la doctrina jurisprudencial que los fue exponiendo.

En segundo lugar, destaca la diversidad de diligencias y su alcance y proyección de uso de cara al futuro. Diligencias como la consistente en el registro remoto de un ordenador, el empleo de grabaciones en el exterior mediante el empleo de drones o sistemas similares, o la grabación de comunicaciones orales en el exterior, son diligencias que en la actualidad son posibles de realizar gracias al avance de la tecnología. En todo caso su uso no está generalizado y por eso es necesario que se vayan empleando para que de este modo se pueda conocer el parecer judicial sobre las normas que las regulan, perfilando su modo de ejecución, etc. Además, las implicaciones del contenido de estas diligencias en el ámbito procesal penal sugieren su estudio desde el punto de vista de su valoración durante la instrucción y el enjuiciamiento.

En tercer lugar, destaca el carácter innovador de algunas de las medidas introducidas en el texto de la LECrim, por ejemplo, las grabaciones de imágenes en espacios públicos, la localización de un determinado sujeto, el registro de dispositivos de almacenamiento masivo de información y datos, la intervención remota de un equipo informático, con lo que resulta claro que el texto legal «*se ha lanzado hacia nuevos horizontes hasta ahora en buena parte inescrutados*»[104].

Este nuevo conjunto de diligencias de investigación electrónicas también plantea numerosos interrogantes, pese al alto grado de detalle que alcanza la nueva regulación[105].

---

[104] Cfr. RODRÍGUEZ LAINZ, José Luis. *El secreto de las comunicaciones y su interceptación legal. Adaptado a la Ley Orgánica 13/2015, de reforma de la Ley de Enjuiciamiento Criminal*. Sepin, Madrid, 2016. Pág. 50. El autor destaca la novedad e importancia de la nueva legislación, y pone algunos ejemplos prácticos de hasta donde se extiende la nueva facultad de intervención de datos y comunicaciones basados en equipos, artefactos y dispositivos que se emplean en la actualidad con frecuencia.

[105] No obstante, no puede decirse que la nueva regulación, con toda su amalgama de nuevos tipos de diligencias, de indudable necesidad, esté exenta de problemas interpretativos de gran calado. Así a título de mero ejemplo de las importantes cuestiones que se plantean respecto de la actual regulación, de la intervención de las comunicaciones telefónicas y telemáticas contenida los arts. 588 ter, a-i, basta con examinar el Auto de 6 de abril de 2016 dictado por la AP de Tarragona (Sección 4º). Ponente: Don Javier Hernández García. En dicho auto se formula una cuestión prejudicial al TJUE mediante la que el tribunal se pregunta acerca de la duda interpretativa que se le ocasiona al aplicar el art. 579.1 LEcrim, puesto en relación con el art. 588 ter apartado a, de la misma norma legal. El último precepto mencionado alude a la necesaria concurrencia de presupuestos exigidos en el art. 579.1 para poder intervenir

En consecuencia, se ha pasado de tener un solo artículo, que se aplicaba a casi todo lo que tuviera que ver con el empleo de la tecnología, a contar con una regulación detallada para cada medida. También es destacable que se hayan regulado unos presupuestos comunes para todas las diligencias (Capítulo IV, arts. 588 bis a) a 588 bis k LECrim), así como unos requisitos específicos para algunas de dichas diligencias de investigación.

Existen otras normas que, fuera de este capítulo, también son exigibles con carácter general. Es el caso del art. 579 bis, relativo a los datos que se obtienen en un proceso distinto, o los hallazgos casuales, que son de aplicación indistinta a todas las diligencias de investigación en las que se trata de proteger el art. 18 de la CE, dado que así es exigido por el contenido del art. 588 bis, i LECrim.

---

comunicaciones telefónicas y telemáticas, o que se trate de delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación. La pregunta que se realiza la Audiencia Provincial de Tarragona es si la gravedad del delito como criterio justificador de la interceptación de las comunicaciones sólo puede establecerse en relación con la pena a imponer por el delito, o si además puede tenerse en consideración la conducta delictiva y el nivel de lesividad de en los bienes jurídicos afectados. Además, también pregunta si en todo caso el umbral de gravedad establecido en la pena de tres años de prisión es bastante. Todo ello se pone en relación con el contenido de los arts. 7 y 8 del CDFUE en unión al art. 8 del CEDH. La respuesta a esta cuestión prejudicial fue informada por el Abogado General el día 3 de mayo de 2018; puede consultarse en el enlace: http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130da99c725d9236648f1bbaee6fd910f3336.e34KaxiLc3eQc40LaxqMbN4Pb3eNe0?text=&docid=201707&pageIndex=0&doclang=ES&mode=req&dir=&occ=first&part=1&cid=219984. En su informe, el Abogado General llega a la conclusión de que en el caso que se ha cuestionado se da una *«injerencia en los derechos fundamentales garantizados por la Directiva y por la Carta que no alcanza un nivel de gravedad suficiente para que dicho acceso deba reservarse a los casos en que el delito sea grave».* La conclusión que se extrae de la opinión del abogado general es que es conforme con el espíritu de las normas protectoras de los derechos fundamentales en Europa, la consideración de la gravedad bajo el prisma de la alarma social debe estar amparada en penas que alcancen el umbral legal nacional para considerar el delito como grave, porque de no hacerse no se justifica la injerencia en el derecho fundamental al secreto de las comunicaciones. Finalmente, la cuestión la resolvió la sentencia de la Gran Sala del Tribunal de Justicia de la UE de fecha 2 de octubre de 2018. La sentencia dictada en el asunto C207/2016 aporta en los considerandos 51 y 53 un criterio interpretativo. Conforme al primero *«el acceso de las autoridades públicas a estos datos constituye una injerencia en el derecho fundamental al respeto de la vida privada, consagrado en el artículo 7 de la Carta, incluso a falta de circunstancias que permitan calificar esta injerencia de «grave» y sin que sea relevante que la información relativa a la vida privada de que se trate tenga o no carácter sensible o que los interesados hayan sufrido o no inconvenientes en razón de tal injerencia. Tal acceso también constituye una injerencia en el derecho fundamental a la protección de los datos personales garantizado por el artículo 8 de la Carta, puesto que constituye un tratamiento de datos personales*», lo que significa que el acceso a datos es una injerencia en un derecho fundamental. El considerando 53 sobre la gravedad viene a decir que *«por lo que se refiere al objetivo de la prevención, investigación, descubrimiento y persecución de delitos, procede observar que el tenor del artículo 15, apartado 1, primera frase, de la Directiva 2002/58 no limita este objetivo a la lucha contra los delitos graves, sino que se refiere a los «delitos» en general»*. En todo caso los considerandos 56 y 57 cierran la cuestión fijando que *«En efecto, conforme al principio de proporcionalidad, en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos solo puede justificar una injerencia grave el objetivo de luchar contra la delincuencia que a su vez esté también calificada de «grave»».* Por su lado el siguiente dice, *«En cambio, cuando la injerencia que implica dicho acceso no es grave, puede estar justificada por el objetivo de prevenir, investigar, descubrir y perseguir «delitos» en general».* Por lo tanto y pese a que no se responde estrictamente a la cuestión que se le planteó, si que se obtiene un criterio de interpretación, conforme al cual cuando la injerencia en los derechos es grave el delito tiene que ser grave también. El CP en su artículo 13, define como delitos graves las infracciones castigadas con pena grave y según el art. 33 del CP considera como penas graves la prisión superior a 5 años. En suma, cuando el art. 579.1 LECrim habla de delitos dolosos castigados con más de 3 años de prisión (también en los 588 ter a) y 588 quáter b), este tipo de delitos no legitimaría el acceso a los datos de tráfico cuando dicha injerencia sea grave porque a tenor del art. 13 CP no son delitos graves, al igual que los cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o de la comunicación o servicio de comunicación del 588 ter a) y 588 septies a) que solamente justificarían una injerencia grave si estuvieran castigados con pena de prisión superior a 5 años.

La evidente heterogeneidad que presentan las distintas diligencias reguladas en la LECrim permite afrontar una propuesta de sistematización y clasificación de estas, que pueda ayudar a su mejor comprensión, sobre todo porque una lectura de todas ellas revela que las nuevas diligencias parecen estar diseminadas por el capítulo sin un orden claro. La Fiscalía general del Estado destaca que la ubicación sistemática de los principios generales aplicables a todas las medidas, y la regulación de cada una de ellas presenta problemas de ubicación, lo que ayuda a justificar la necesidad de realizar una ordenación y clasificación[106].

Por lo anterior es por lo que procede adelantar y elaborar una propuesta de clasificación de esas diligencias, porque la aparente falta de orden se intensifica a partir del Capítulo IV del Título VIII, lo que conduce a preguntarse cuáles son las razones por las que las diligencias se presentan del modo en que lo hacen, llegando a generar cierta confusión, por lo que es útil manejar un adecuado criterio de clasificación para ordenar la panoplia de diligencias de investigación que el legislador ha puesto a disposición de las investigaciones criminales.

La forma de llevar a cabo la propuesta de sistemática y clasificación de las diligencias contenidas en el texto legal puede hacerse sin abandonar el tenor literal de la ley. El texto legal aporta algunas pautas que permiten realizar la siguiente propuesta de clasificación y sistematización. En concreto esas pautas se encuentran en la Exposición de Motivos de la Ley Orgánica 13/2015 [107].

La lectura de la Exposición permite vislumbrar la preocupación del legislador sobre la «*relación con algunos de los derechos constitucionales que puedan ser objeto de limitación en el proceso penal*». Estos derechos constitucionales se concretan más tarde, a lo largo del texto de la Exposición en los referentes a «*la privacidad del investigado*» [108], a la «*injerencia del Estado en las comunicaciones particulares*»[109], a la «*incidencia que en la intimidad de cualquier persona puede tener el conocimiento por los poderes públicos de su ubicación espacial*», y, por último, a modo de resumen, la «*afectación a ninguno de los derechos fundamentales del artículo 18 de nuestro texto constitucional*».

Lo anterior permite concluir que el legislador ordena y clasifica las diligencias de investigación atendiendo a la limitación que cada concreta medida conlleva en cada uno de los derechos fundamentales relacionados en el art. 18 CE. Esta razón[110] justifica que el Título VIII tenga como

[106] Circular de la Fiscalía General del Estado 1/2019, de 6 de marzo. Pág. 3.
[107] Sobre todo es necesaria la lectura del apartado IV de la Exposición de Motivos de la LO 13/2015.
[108] Párrafo primero, in fine, del apartado IV de la Exposición de Motivos de la LO 13/2015.
[109] Párrafo séptimo, in fine, del apartado IV de la Exposición de Motivos de la LO 13/2015.
[110] A la que también puede unirse el reconocimiento del derecho al propio entorno virtual que se vio en el apartado anterior siguiendo los razonamientos que se dieron allí.

rúbrica: «*medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución*».

Por otra parte, la exigencia de un conjunto mayor o menor de requisitos y presupuestos para adoptar una medida limitadora de los derechos del art. 18 CE puede servir también como criterio clasificatorio autónomo. Se trataría de una clasificación que permitiría delimitar aquellas diligencias a las que basta la aplicación de los presupuestos comunes, de aquellas otras a las que además le son exigibles requisitos y presupuestos específicos.

Como puede constatarse cabe la posibilidad de realizar la ordenación de estas diligencias atendiendo a diversos criterios, por lo que en los apartados siguientes se procederá a esbozar una propuesta dirigida a este fin.

1.1. Clasificación en función de la afectación del tipo de derecho constitucional que se regule y contenga en el art. 18 CE.

El tipo de derecho afectado por la medida de investigación sirve como primer criterio para clasificar las diligencias de investigación contenidas en el Título VIII de la LECrim. También puede servir como criterio sistematizador el grado de afectación sobre un determinado derecho fundamental de entre los contemplados en el art. 18 CE.

En lo que se refiere al primero de los criterios apuntados, hay que partir del hecho de que el derecho fundamental que en cada caso se trate, no siempre es igualmente afectado por la medida de investigación. La limitación del derecho puede ser completamente pura, es decir, puede afectar sólo y únicamente a uno de los derechos fundamentales contenidos en el art. 18 CE (por ejemplo, afectar sólo al secreto de las comunicaciones o sólo a la intimidad), por el contrario, puede tratarse de una afectación mixta, en la que hay más de uno de estos derechos implicados. Esto último quiere decir que la decisión de adoptar una determinada diligencia de investigación puede conllevar la limitación de más de uno de los derechos fundamentales del art. 18 CE (por ejemplo, afectar al mismo tiempo a la intimidad domiciliaria y a la intimidad personal).

Este tratamiento mixto y conjunto de derechos constitucionales, producido durante la práctica de una diligencia de investigación ha sido un hecho admitido por el Tribunal Supremo y el Tribunal

Constitucional[111], constituyendo el origen del derecho al propio "entorno virtual", que más arriba se analizó, y al que se le dio la misma protección constitucional que si se tratara de uno sólo[112].

La enumeración de las diligencias que conllevan la afectación pura de derechos fundamentales del art. 18 de la CE, son las siguientes:

- la diligencia consistente en la entrada y registro en lugar cerrado, que se regula en el Capítulo I del Título VIII (arts. 545 a 572 LECrim) porque su realización puede relacionarse únicamente con la afectación del contenido del derecho a la inviolabilidad del domicilio, que se recoge en el art. 18.2 CE.

- la diligencia de registro de libros y de papeles, que se contiene en el Capítulo II del mismo Título (arts. 573 a 578 LECrim), ya que sólo guarda relación con la afectación al contenido del derecho a la intimidad que se contiene en el art. 18.1 CE.

- la diligencia de investigación que consiste en la detención y apertura de la correspondencia escrita y telegráfica, que se regula en el art. 579 al art. 588 LECrim, porque guarda relación tan sólo con el contenido del derecho al secreto de las comunicaciones escritas, que se contiene en el art. 18.3 CE.

Ahora bien, hay que matizar que el derecho al secreto de las comunicaciones es susceptible de ser desglosado en función de la concreta modalidad comunicativa de que se trate en cada caso. Las comunicaciones entre sujetos, que son susceptibles de ser investigadas, pueden ser escritas y también pueden ser orales. El paradigma de la primera modalidad es la intervención de la correspondencia escrita, mientras que el de la segunda es la intervención telefónica. Así, la limitación a la que puede verse sometido el derecho al secreto de las comunicaciones puede realizarse por la aplicación de la diligencia del Capítulo III LECrim, y también por las diligencias

[111] STC 173/2011, de 7 de noviembre. Ponente: Don Eugenio Gay Montalvo. Por no resultar redundante, parte del contenido de esta sentencia viene desarrollado en nota posterior.

[112] Cabe citar además de alguna otra más antigua que será objeto de comentario las STS 97/2015, de 24 de febrero. Ponente: Don Juan Ramón Verdugo y Gómez de la Torre. Fundamento de derecho cuarto, página 15; la STS 786/2015, de 4 de diciembre. Ponente: Don Manuel Marchena Gómez. Fundamento de derecho primero, página 10; la STS 204/2016, de 10 de marzo. Ponente: Don Cándido Conde Pumpido-Tourón; fundamento de derecho séptimo, página 10; y la STS 287/2017, de 19 de abril. Ponente: Don Manuel Marchena Gómez; fundamento de derecho segundo, página 4. Todas las sentencias recogen la consolidada doctrina que convierte la suma de varios de los derechos protegidos en el artículo 18 CE en un derecho de nuevo cuño denominado derecho al propio entorno virtual, en el que se protege la suma de los aspectos del sujeto investigado cuando participa en las diversas dimensiones que ofrecen las nuevas tecnologías de la información y la comunicación.

contenidas en el Capítulo V LECrim, aunque en este segundo caso se refiere a la interceptación de las comunicaciones que se desarrollen de forma telefónica y telemática. En ambos casos se sigue estando ante una limitación pura del derecho al secreto de las comunicaciones, por cuanto es el haz de un mismo derecho el que está siendo limitado, sin que lo hagan otros derechos distintos a ese al mismo tiempo.

La regulación de la modalidad de intervención en las comunicaciones a través de vías telefónicas o telemáticas es mucho más compleja que el registro de papeles y de documentos. Solo basta comparar ambas regulaciones para constatarlo.

La intervención de las comunicaciones orales se regula dentro del Capítulo V, del Título VIII, siendo la Sección Primera la que contiene los aspectos o disposiciones generales -arts. 588 ter a al art. 588 ter i de la LECrim- ; la Sección Segunda regula cómo se han de incorporar al proceso penal todos los datos de tráfico de esos procesos de comunicación oral, - sólo se contempla la cuestión dentro del contenido del art. 588 ter j LECrim- ; la Sección Tercera, se dedica a regular el acceso a los datos que permiten determinar el usuario y el terminal que se emplea en el proceso de comunicación, o bien el dispositivo que se emplea para conectarse a un proceso de comunicación -arts. 588 ter k al art. 588 ter m LECrim-. Este amplio conjunto de subdivisiones en la ley llega a despistar y nos hace olvidar que estemos sólo ante el modo de limitar un solo derecho. La razón de que la limitación al derecho al secreto de las comunicaciones telefónicas y telemáticas sea desglosada en varios apartados de la ley de manera separada, descansa principalmente en el modo de entender el proceso de comunicación, que es considerado como un acto integrado por numerosos componentes que van desde los intervinientes a los datos que genera la comunicación misma.

En todo caso, la práctica de ambas diligencias de intervención de comunicaciones, bien sea la escrita, o sea la oral, exige que se preste observancia del contenido del art. 579 LECrim, que es la norma que fija los presupuestos generales que deben concurrir antes de que se produzca toda limitación en el derecho al secreto de las comunicaciones. No obstante, no debe olvidarse que se está en los dos supuestos ante la limitación del mismo derecho, y ello con independencia del medio empleado para acceder al contenido de la comunicación.

La segunda diligencia de limitación pura del derecho al secreto de las comunicaciones es la consistente en la grabación de comunicaciones orales empleando medios técnicos que permitan hacerlo. La Circular de la Fiscalía General del Estado 3/2019, de 6 de marzo, comparte esta misma afirmación, considerando que su fundamento se encuentra en la propia normativa procesal en la que *«el legislador confiere a esta regulación la protección propia del derecho fundamental al secreto*

de las comunicaciones»[113]. Se regula en el Capítulo VI, -arts. 588 quater a hasta el art. 588 quater e LECrim-. Esta modalidad de investigación electrónica no comparte con las diligencias de los capítulos III y V LECrim, ya mencionadas, la obligación de atenerse sólo al contenido del art. 579 LECrim, sino que cuenta con sus propios presupuestos específicos.

Los requisitos que exige esta otra diligencia son mucho más restrictivos porque se trata de una medida que la doctrina ha considerado como *«de un potencial invasivo muy superior al que tienen las intervenciones telefónicas»*[114] y que *«puede tener efectos colaterales en personas que convivan con los sujetos investigados y que nada tengan que ver con el hecho delictivo»*[115] . Estos aspectos son los que resultan decisivos a la hora de reforzar las exigencias, presupuestos y requisitos exigibles para poder acordar la diligencia. La misma requiere una insoslayable autorización judicial y queda circunscrita a la investigación de determinados delitos de innegable gravedad, tales como delitos de terrorismo o los cometidos mediante una organización criminal. La diligencia afecta en puridad al derecho al secreto de las comunicaciones, aunque es susceptible de ser ampliada de forma que también recoja imágenes o se recaben las conversaciones dentro de lugar cerrado, siendo que en esos casos, claramente determinados por la solicitud que se formule por los agentes encargados de la investigación, la diligencia pasaría a ser de carácter mixto, si hay más derechos afectados, como la intimidad, la inviolabilidad del domicilio o cualquier otro. En cierto modo esta diligencia, en su modalidad de afectación mixta, presenta ciertas similitudes con la diligencia de registro remoto de equipos informáticos, en tanto que los mismos derechos pueden ser afectados por la realización tanto de una como de otra.

El segundo grupo de diligencias de investigación, agrupadas en torno al criterio delimitador de la afectación a más de uno de los derechos fundamentales del art. 18 CE, por lo tanto, la afectación de modo mixto, son las que a continuación se relacionan:

---

[113] Se indica expresamente en el apartado 2 de la Circular, denominada Alcance de la medida.

[114] Cfr. RICHARD GONZÁLEZ. Manuel. «Conductas susceptibles de ser intervenidas por medidas de investigación electrónica. Presupuestos para su autorización Manuel». *Diario La Ley*, Nº 8808, 21 de Julio de 2016. LA LEY 5735/2016. Pág. 6

[115] Cfr. BUENO DE MATA, Federico. «Comentarios y reflexiones sobre la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica». Diario La Ley, Nº 8627, 19 de Octubre de 2015. LA LEY 5958/2015. Pág. 4.

- la diligencia que se contiene en el Capítulo VII LECrim que regula el empleo de medios técnicos que permiten captar la imagen, la localización y hacer un seguimiento del sujeto investigado (arts. 588 quinquies a, hasta 588 quinquies c, de la LECrim).

Con la práctica de la diligencia del art. 588 quinquies a, se afecta, al mismo tiempo, el derecho a la intimidad y a la propia imagen. La diligencia lo que permite es grabar a una persona dentro de un espacio público, como se aprecia en el párrafo 1 del art. 588 quinquies, apartado a. Esto claramente afecta a su imagen por cuanto la misma es tomada sin el consentimiento del afectado, pero con la clara vocación de ser la *«constancia documental de lo que el investigador está viendo»*[116], al tiempo que permite acreditar el lugar en el que se encontraba el investigado y con qué personas se estaba relacionando en un determinado momento. Estas acciones se relacionan claramente tanto con la imagen del investigado, tomada sin la concurrencia de su voluntad, como con su intimidad, en la medida en que se conoce el lugar en el que está o con quien se relaciona, sin su consentimiento. Esta diligencia admite otras modalidades, como lo es el seguimiento y localización mediante artefactos técnicos, prevista en el art. 588 quinquies b LECrim, que permiten la localización de la persona, bien mediante la colocación de uno de estos artefactos en un determinado objeto (lo que conlleva localizar mediante el empleo de una baliza de geolocalización, desde un turismo a una embarcación, por poner un ejemplo). En este concreto caso se afecta principalmente a la intimidad en tanto que se conoce el paradero de la persona sometida a la diligencia, sin su autorización. Pero incluso se admite la posibilidad de que esta diligencia se utilice relacionada con diligencias ya existentes como la consistente en la entrega vigilada, lo que también admite la doctrina [117], lo que conllevaría admitir la afectación tanto de la intimidad como de otros derechos como por ejemplo el derecho al secreto de las comunicaciones.

- la diligencia regulada en el Capítulo VIII LECrim, consistente en el acceso a los dispositivos de almacenamiento masivo de la información (arts. 588 sexies a, hasta el art. 588 sexies c LECrim).

[116] Cfr. JIMÉNEZ SEGADO, Carmelo y PUCHOL AIGUABELLA, Marta. «Las medidas de investigación tecnológica limitativas de los derechos a la intimidad, la imagen, el secreto de las comunicaciones y la protección datos». Diario La Ley, Nº 8676, 7 de Enero de 2016. . Pág. 8.

[117] Vid. LÓPEZ YAGÜES, Verónica. «Investigación de delitos sobre tráfico de sustancias y bienes ilícitos: circulación y entrega vigilada y dispositivos de seguimiento». Diario La Ley, Nº 9095, Sección Doctrina, 7 de Diciembre de 2017, LA LEY *17244/2017*. Pág.10.

- la diligencia contemplada en el Capítulo IX LECrim referente al acceso remoto a equipos informáticos (arts. 588 septies a, hasta el art. 588 septies c LECrim).

En el caso de las dos últimas diligencias relacionadas se afecta, al mismo tiempo, a un conjunto de derechos fundamentales: la intimidad, el derecho al secreto de las comunicaciones, el derecho a la propia imagen, etc. Se trata de las dos diligencias que más ejemplifican la protección del «*derecho al propio entorno virtual*»[118], en tanto que conllevan la limitación de varios derechos de rango constitucional conjuntamente[119].

[118] La STS 342/2013, de 17 de abril. Ponente: Don Manuel Marchena Gómez, en el fundamento de derecho 8º, página 22 hace alusión a la necesaria autorización judicial para acceder a un ordenador, poniendo de manifiesto que «s*on muchos los espacios de exclusión que han de ser garantizados»*. Se alude a que un ordenador contiene diversos datos y por ello «l*a ponderación judicial de las razones que justifican…el sacrificio de los derechos de los que es titular el usuario del ordenador, ha de hacerse sin perder de vista la multifuncionalidad de los datos que se almacenan en aquel dispositivo. Incluso su tratamiento jurídico puede llegar a ser más adecuado si los mensajes, las imágenes, los documentos y, en general, todos los datos reveladores del perfil personal, reservado o íntimo de cualquier encausado, se contemplan de forma unitaria. Y es que, más allá del tratamiento constitucional fragmentado de todos y cada uno de los derechos que convergen en el momento del sacrificio, existe un derecho al propio entorno virtual. En él se integraría, sin perder su genuina sustantividad como manifestación de derechos constitucionales de nomen iuris propio, toda la información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos. Surge entonces la necesidad de dispensar una protección jurisdiccional frente a la necesidad del Estado de invadir, en las tareas de investigación y castigo de los delitos, ese entorno digita*l».
La propia sentencia distingue, como lo hace el actual art. 588 series a) entre los derechos a la inviolabilidad de las comunicaciones y a la intimidad, exigiendo autorización para acceder al domicilio en el que aquellos dispositivos se encuentran instalados y otra diversa para acceder a estos últimos. Sigue diciendo la sentencia: «*La STC 173/2011, 7 de noviembre, recuerda la importancia de dispensar protección constitucional al cúmulo de información personal derivada del uso de los instrumentos tecnológicos de nueva generación».* Allí puede leerse el siguiente razonamiento: *«si no hay duda de que los datos personales relativos a una persona individualmente considerados, a que se ha hecho referencia anteriormente, están dentro del ámbito de la intimidad constitucionalmente protegido, menos aún pueda haberla de que el cúmulo de la información que se almacena por su titular en un ordenador personal, entre otros datos sobre su vida privada y profesional (en forma de documentos, carpetas, fotografías, vídeos, etc.) -por lo que sus funciones podrían equipararse a los de una agenda electrónica-, no sólo forma parte de este mismo ámbito, sino que además a través de su observación por los demás pueden descubrirse aspectos de la esfera más íntima del ser humano. Es evidente que cuando su titular navega por Internet, participa en foros de conversación o redes sociales, descarga archivos o documentos, realiza operaciones de comercio electrónico, forma parte de grupos de noticias, entre otras posibilidades, está revelando datos acerca de su personalidad, que pueden afectar al núcleo más profundo de su intimidad por referirse a ideologías, creencias religiosas, aficiones personales, información sobre la salud, orientaciones sexuales, etc»*. La Sentencia continúa su razonamiento indicando que «*estos datos….si se analizan en su conjunto*, *configuran todos ellos un perfil altamente descriptivo de la personalidad de su titular, que es preciso proteger frente a la intromisión de terceros o de los poderes públicos*. *A esto debe añadirse que el ordenador es un instrumento útil para la emisión o recepción de correos electrónicos, pudiendo quedar afectado en tal caso, no sólo el derecho al secreto de las comunicaciones del art. 18.3 CE (por cuanto es indudable que la utilización de este procedimiento supone un acto de comunicación), sino también el derecho a la intimidad personal (art. 18.1 CE), en la medida en que estos correos o email, escritos o ya leídos por su destinatario, quedan almacenados en la memoria del terminal informático utilizado. Por ello deviene necesario establecer una serie de garantías frente a los riesgos que existen para los derechos y libertades públicas, en particular la intimidad personal, a causa del uso indebido de la informática así como de las nuevas tecnologías de la información*».
[119] La misma STS 342/2013 citada en la nota anterior sigue diciendo sobre este particular aspecto que los datos pueden ser: *«irrelevantes o livianos si se consideran aisladamente, pero si se analizan en su conjunto, una vez convenientemente entremezclados, no cabe duda que configuran todos ellos un perfil altamente descriptivo de la personalidad de su titular, que es preciso proteger frente a la intromisión de terceros o de los poderes públicos, por*

1.2. Clasificación atendiendo a los requisitos y presupuestos legales exigibles para la adopción de la medida.

Un segundo criterio que sirve para clasificar las diligencias previstas en el Título VIII de la LECrim es el que permite dividirlas en función de las exigencias y requisitos que son determinantes para su adopción.

La nueva regulación procesal exige la concurrencia de requisitos que justifican la adopción de una diligencia de investigación. La decisión implica limitar el contenido de un derecho fundamental que, o bien es algún derecho específico del art. 18 CE, o bien es una amalgama de estos. Los requisitos que se exigen para ello se erigen en presupuesto de legalidad de la medida. No se trata de una mera cuestión formal, sino que la multiplicación de dichos requisitos y exigencias para la adopción de estas nuevas diligencias de investigación constituyen una auténtica seña de identidad que permiten diferenciar claramente entre la regulación anterior a la reforma y la actual, y constituyen la expresión del necesario respeto a las garantías procesales y constitucionales que debe conllevar necesariamente la limitación o afectación de los derechos fundamentales.

En la regulación anterior a la reforma, era el Juez el que determinaba, valorándolo y razonándolo en el auto habilitante, los requisitos y presupuestos que estimaba necesarios a los efectos de acordar una medida, rigiéndose únicamente por los criterios conformados por la jurisprudencia, sin respaldo legal. Por el contrario, la nueva regulación resulta mucho más extensa, muy profusa y exigente en la determinación de los requisitos para acordar una medida limitativa de derechos fundamentales.

Es ese último aspecto el que permite distinguir las diligencias de investigación en función de que se exija una mayor o menor cantidad de requisitos y de presupuestos para su adopción. Por eso, siguiendo este segundo criterio de clasificación de diligencias, las mismas pueden ser divididas entre aquellas que:

---

cuanto atañen, en definitiva, a la misma peculiaridad o individualidad de la persona. A esto debe añadirse que el ordenador es un instrumento útil para la emisión o recepción de correos electrónicos, pudiendo quedar afectado en tal caso, no sólo el derecho al secreto de las comunicaciones del art. 18.3 CE (por cuanto es indudable que la utilización de este procedimiento supone un acto de comunicación), sino también el derecho a la intimidad personal (art. 18.1 CE), en la medida en que estos correos o email, escritos o ya leídos por su destinatario, quedan almacenados en la memoria del terminal informático utilizado. Por ello deviene necesario establecer una serie de garantías frente a los riesgos que existen para los derechos y libertades públicas, en particular la intimidad personal, a causa del uso indebido de la informática así como de las nuevas tecnologías de la información».

1) exigen para su adopción el respeto a los requisitos generales de cualquier intervención: es decir, ser adoptada mediante resolución judicial, debidamente motivada atendiendo a los criterios de proporcionalidad, necesidad, etc. Entre ellas quedarían así encuadradas la totalidad de las diligencias contenidas en el Título VIII de la LECrim.

2) las que requieren, además de lo anterior, sus propios presupuestos y exigencias, siendo incluidas en este caso las relativas a la detención y apertura de la correspondencia escrita y telegráfica (Capítulo III LEcrim) y la interceptación de las comunicaciones telefónicas y telemáticas (Capítulo V LEcrim). Para la adopción de cualquiera de ellas, se exige la concurrencia de los presupuestos del art. 579.1 LECrim. Por su parte, la diligencia consistente en el registro remoto de equipos informáticos (Capítulo IX LECrim) también exige que concurra, con anterioridad a su adopción, los presupuestos específicos contenidos en los artículos de la ley dedicados a su regulación, los cuales, una vez verificados, deberían continuar adicionándose a las demás exigencias comunes a todas las diligencias de investigación electrónica.

Hay otros posibles criterios clasificatorios que pueden ser empleados para sistematizar las distintas diligencias. En este sentido, se pueden proponer como criterios, atender al medio concreto que contiene la información a la que se desea acceder (una agenda de papel, una comunicación oral que está grabada en un smartphone o los datos electrónicos almacenados en un disco externo, entre otros), para sustentar una división de las diligencias de investigación que afectan o limitan derechos fundamentales del art. 18 CE (por ejemplo, el registro de papeles o el registro de conversaciones telefónicas, o el registro de dispositivos de almacenamiento masivo de información). Otro criterio taxonómico puede ser atender a según que sea necesario o no la intervención de terceros para conseguir realizar de manera efectiva la realización de la diligencia, por ejemplo las diligencias que exigen la intervención de las compañías telefónicas para que éstas aporten determinados datos de comunicación, o las diligencias de registro remoto de equipos que impone a terceros la obligación de prestar su ayuda en todo lo necesario a los efectos de poder obtener los datos esenciales para la investigación criminal emprendida, etc.

El resultado de este proceso de clasificación permite, al referirse a cada diligencia, mostrar las características que las definen y que al mismo tiempo las delimitan de las demás. Por ejemplo, a la hora de describir las dos diligencias de investigación en las que se centra este estudio, podrían definirse como diligencias de carácter mixto, al afectar con su adopción a varios derechos fundamentales a la vez.

Por otro lado, y con la finalidad de deslindarlas entre sí, cabe decir que mientras la diligencia de acceso a un dispositivo de almacenamiento de información sólo requiere que concurran los estándares generales exigibles a todas las diligencias de investigación en general, la diligencia de acceso remoto a un equipo informático exige unos requisitos y presupuestos especiales. Esta segunda es una diligencia más restringida, que sólo puede acordarse y llevarse a cabo cuando concurran los aspectos tanto generales como específicos de manera insoslayable.

2. Principios rectores aplicables a cualquier medida de intervención.

2.1. Introducción.

La totalidad de las diligencias contenidas en el Título VIII de la LECrim están sometidas al cumplimiento de unas notas o exigencias comunes que deben concurrir con carácter previo a su adopción.

El hecho de que la nueva regulación de las diferentes diligencias de investigación que afectan a los derechos del art. 18 CE cuente con una clara y amplia descripción de los requisitos necesarios para ser acordadas, es algo que contrasta con la regulación anterior. Pero si lo anterior es destacable, no lo es menos el que la ley contenga los criterios que permiten al Juez encargado de adoptarlas, valorar si la práctica de cada diligencia que se le solicita es adecuada y ajustada a las circunstancias. La norma fija, con carácter general para buena parte de las diligencias de investigación, la necesidad de motivar la concurrencia de dichos principios, que califica de rectores. Se trata de criterios, que no son nuevos, y que han ido siendo establecidos por parte de la jurisprudencia en orden a determinar la procedencia y legalidad de cada medida de investigación que le era sometida a consideración. En general puede decirse que esa jurisprudencia se fue desarrollando, sobre todo, en el ámbito del derecho al secreto de las comunicaciones, principalmente las telefónicas, pero también en el ámbito de las diligencias de registros domiciliarios, entregas vigiladas de estupefacientes, etc. El legislador lo que ha hecho ha sido convertir en norma jurídica todos esos criterios y principios jurisprudenciales, que ahora se convierten en aspectos de necesaria observancia y de obligada valoración. Quedan por lo tanto consignados en la ley, y resultan por ello de obligada aplicación al supuesto que se someta.

Los presupuestos de hecho (tanto generales, como específicos de cada diligencia), los requisitos de forma, y estos principios rectores, se configuran como exigencias que deben estar siempre presentes y que son necesarios. Sólo una vez que por parte del Juez instructor se constata que concurren no

sólo los requisitos y exigencias fácticas, sino que además también confluyen en el supuesto concreto los principios rectores contenidos en el art. 588 bis a LECrim, es cuando será posible la adopción de la diligencia solicitada, despejando con ello cualquier duda sobre la legalidad de esta.

El inicio del estudio de los requisitos comunes a las diligencias de investigación electrónica de este trabajo ha de comenzarse por el contenido de todos estos principios rectores que guían el examen previo a cualquier adopción de las medidas de intervención. El análisis debe enmarcarse en la legislación positiva, y completarse con el parecer de la doctrina y la jurisprudencia sobre su contenido.

El Título VIII LECrim, cuya rúbrica es *«De las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución»*, es el que contiene toda esta nueva ordenación sobre esta materia que, como aprecia la doctrina, *«ve sustancialmente modificada tanto su distribución como regulación»*[120] que existía con anterioridad a la reforma de 2015. Este Título VIII de la LECrim cuenta con diez capítulos, que regulan las distintas clases de diligencias de investigación relacionadas tanto con la intervención del proceso de comunicación escrito, como con el oral por vía telefónica, y también telemática; también regula el acceso al domicilio o a otros lugares cerrados; y contiene la regulación que se refiere a cualesquiera otros métodos de investigación que guarden relación con la necesaria cobertura jurídica que debe brindarse a la intervención del Estado en los derechos del art. 18 CE de los ciudadanos.

Los capítulos que se contienen dentro del Título VIII son los siguientes:

I. De la entrada y registro en lugar cerrado.

II. Del registro de libros y papeles.

III. De la detención y apertura de la correspondencia escrita y telegráfica.

IV. Disposiciones comunes a la interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de las comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos de equipos informáticos.

[120] Cfr. GARCÍA SAN MARTÍN, Jerónimo. «Consideraciones en torno al anteproyecto de Ley Orgánica de modificación de la Ley de Enjuiciamiento Criminal para la agilización de la justicia penal, el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas (1)». *Diario La Ley* nº 8468, 28 de enero de 2015. Pág. 8.

V. La interceptación de las comunicaciones telefónicas y telemáticas[121]. Este apartado cuenta a su vez con dos secciones; la primera que está denominada como «*disposiciones generales*», mientras que sección segunda se llama «*incorporación al proceso de datos electrónico de tráfico asociados»*.

VI. Captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos[122].

VII. Utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización[123].

VIII. Registro de dispositivos de almacenamiento masivo de información.

IX. Registros remotos sobre equipos informáticos.

X. Medidas de aseguramiento.

El contenido del Título VIII de la norma procesal penal, junto a las diligencias anteriormente descritas, cuenta en el apartado IV, con una serie de disposiciones comunes a todas ellas. Estas disposiciones, que se analizan a continuación, son fruto, además de la jurisprudencia que las fue desarrollando, del propio contexto temporal en el que estas normas fueron aprobadas. En el momento de la creación de esta norma, había otras leyes en estado de aprobación o ya promulgadas, que abundaban en una clara corriente reformadora dirigida a actualizar las normas existentes, y a reforzar los derechos de los investigados y de las víctimas. Es en ese contexto donde deben situarse e interpretarse las normas que se verán, huyendo de un examen aislado y autónomo de éstas, y orientar el estudio de la ley procesal hacia una interpretación sistemática con aquellas otras leyes dictadas en esos momentos.

En el año dos mil quince en materia penal sustantiva se produjo entre otras reformas, la del Código penal y la aprobación del Estatuto de la víctima del Delito. En materia procesal penal remarca la doctrina que se aprobaron leyes que no afectaban a derechos fundamentales y otras que sí, *«como el estatuto del investigado y las diligencias de investigación tecnológica, y …. las de índole procesal, entre las que se encuentran las medidas de agilización de la justicia penal y otras garantías como*

[121] Se trata de una diligencia cuyo contenido además de por las normas reguladoras se ha visto interpretado por la Fiscalía General del Estado en su Circular 2/2019 , de 6 de marzo.
[122] Siguiendo la nota anterior, esta diligencia se ha interpretado en la CFGE 3/2019, de 6 de marzo.
[123] Ver el contenido de la Circular de la Fiscalía General del Estado 4/2019, de 6 de marzo.

el proceso monitorio penal, la generalización de la segunda instancia y la ampliación del recurso de revisión» [124].

De manera más concreta pueden citarse entre las normas de aprobación próxima a la que aquí se estudia, la Ley Orgánica 1/2015, de 30 de marzo y la Ley Orgánica 2/2015, de 30 de marzo, que modifican el Código Penal y, entre otras cosas introduce nuevos tipos penales claramente relacionados con el empleo de los medios tecnológicos, en este sentido se introducen los arts. 197.7, 197 bis, 172 ter, 468.3, que guardan relación con el uso de la tecnología; la Ley 4/2015 de 27 de abril que aprueba el Estatuto de la Víctima se encuadra también en esta actividad legislativa, si bien encaminada a reforzar los derechos de los distintos implicados en la actividad delictiva, concretamente a las víctimas; asimismo, y en esta línea de reforzamiento de derechos cabe mencionar la Ley Orgánica 5/2015, de 27 de abril, en materia de interpretación y traducción y a la información en los procesos penales, que refuerza el conjunto de derechos de los investigados. Por último, cabe mencionar la Ley Orgánica 13/2015 que se analiza en este trabajo.

La aprobación de estas normas nos permite vislumbrar que la actividad legislativa iba dirigida a actualizar las normas penales, tanto sustantivas como procesales, y al mismo tiempo reforzar los derechos de los implicados en la actividad delictiva. Esa actualización, entre otras materias, comprendía la dirigida al ámbito tecnológico, y lo hacía en el derecho penal sustantivo recogiendo tipos penales que emplean en el modo comisivo la tecnología, mientras que en el derecho procesal penal lo hacía actualizando las diligencias de investigación para admitir los medios de averiguación de los delitos usando medios tecnológicos. Por su parte el reforzamiento de derechos comprende no sólo los de carácter constitucional relacionados con el art. 18 CE que ya se han visto, sino también otros derechos con implicación constitucional como el derecho de defensa, los derechos de las víctimas, etc.

En consecuencia, en ese contexto de modernización y puesta al día de las leyes, nacen las diligencias de investigación que se analizan más adelante, y dentro de ese contexto de refuerzo de derechos se contempla la inclusión de los principios rectores que otorgan a toda diligencia un plus de seguridad y de valoración previas que las aleja de cualquier arbitrariedad.

La mayoría de los autores coincidían en señalar que las normas sobre la intervención de las comunicaciones y las demás diligencias de afectación de los derechos del art. 18 CE, exigían una apremiante, necesaria e inaplazable aprobación. España había sido apremiada a hacerlo por distintas

[124] Cfr. GONZÁLEZ MONTES-SÁNCHEZ, José Luis. «Reflexiones sobre el proyecto de Ley Orgánica de modificación de la LECRIM para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica». *Revista electrónica de Ciencia Penal y criminología.* RECPC 17-06 (2015). Pág. 6.

instancias internacionales y por las más altas instancias judiciales nacionales, representadas por el Tribunal Supremo y por el Tribunal Constitucional. Todas coincidían en señalar que la legislación nacional con la que se contaba, el art. 579 LECrim, era claramente insuficiente. Esta raquítica regulación adolecía de una palpable ausencia de supuestos de intervención sobre derechos fundamentales distintos del derecho al secreto de las comunicaciones orales. A su vez, la creciente presencia de la tecnología puso en evidencia, todavía más si cabe, la carencia de toda regulación sobre estos nuevos medios técnicos, que estaba siendo demandada por los Cuerpos y Fuerzas de Seguridad del Estado para el correcto ejercicio de sus funciones de investigación de ilícitos penales[125].

En la Exposición de Motivos del texto de reforma de la Ley, el propio legislador es quien advierte de la necesidad de proceder a la regulación de las medidas que se van desarrollando a lo largo de su texto. Se justifica y se razona acerca de los motivos de esta nueva legislación considerando que «*los flujos de información generados por los sistemas de comunicación telemática advierten de las posibilidades que se hallan al alcance del delincuente, pero también proporcionan poderosas herramientas de investigación a los poderes públicos. Surge así la necesidad de encontrar un delicado equilibrio entre la capacidad del Estado para hacer frente a una fenomenología criminal de nuevo cuño y el espacio de exclusión que nuestro sistema constitucional garantiza a cada ciudadano frente a terceros*»[126].

El legislador pretendía hacer compatible la investigación y persecución de los delitos, con el máximo respeto y cuidado de los derechos constitucionales afectados por la práctica de dicha actividad investigadora, y con tal finalidad incrementó la gama de diligencias de investigación de delitos, otorgando a cada una un marco regulatorio bien definido. Todo ello dentro del ámbito del reforzamiento de derechos que más arriba ha sido esgrimido.

En esta tarea de compatibilizar las nuevas diligencias de investigación tecnológica con la garantía y defensa de los derechos de los ciudadanos, el legislador renunció a la creación de un marco ex novo. No hay duda de que nuestros legisladores podrían haber optado por cualquier otro sistema de regulación de esta materia basado en aspectos y criterios diferentes a los finalmente elegidos, pero

[125] Sentencia del Tribunal Constitucional 145/2014, de 22 de septiembre. Esta sentencia otorgó parcialmente el amparo al recurrente, y estimó que la diligencia mediante la que se acordaron unas medidas de intervención consistentes en las escuchas de conversaciones llevadas a cabo en dependencias de retención (en concreto en unos calabozos), no habían sido ajustadas a derecho, considerando el Tribunal Constitucional que la razón de ello es que no existía cobertura legal alguna que amparase la adopción de la medida, vulnerándose de este modo el principio de reserva de Ley que debe primar en cualquier limitación de derechos fundamentales.

[126] Extraído de la Exposición de motivos, apartado IV, de la ley Orgánica 13/ 2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. Publicado en el Boletín Oficial del Estado número 239, del día 6 de octubre de 2015, sección I, Página 90192.

decidieron ajustarse a los criterios y a los principios que habían venido rigiendo la actuación de los Tribunales de justicia, y que habían sido creados, elaborados y desarrollados por los mismos durante muchos años[127]. El resultado que se ha obtenido ha sido el de elevar a rango de ley la consolidada doctrina jurisprudencial sobre los principios que regían cualquier intervención en estas materias[128].

La doctrina jurisprudencial se ha tornado norma jurídica positiva, siendo la relativa a los presupuestos generales la que se contiene en el Capítulo IV, del Título VIII LECrim, artículos 588 bis a), hasta 588 bis k) de la LECrim.

Estos presupuestos son la trasposición de la doctrina jurisprudencial antes aludida, y su resultado es la elevación a rango de ley de lo que se denominan *«principios rectores»* (art. 588 bis a LECrim). Se trata de principios interpretativos cuya valoración y concurrencia son exigibles para adoptar cualquiera de las nuevas diligencias contempladas en el Título VIII LECrim. De entre ellos se destacan los siguientes:

(i) Necesidad de autorización judicial.

Este requisito ya era exigido desde hacía mucho tiempo. Es la consecuencia del mandato constitucional, que exige que sea el Juez el que limite algunos derechos fundamentales cuando ello proceda. En este sentido cabe decir que los derechos del art. 18 CE no siempre deben ser limitados por un Juez, como forma de salvaguardar su contenido esencial. De hecho, la doctrina jurisprudencial que se refiere a esta intervención judicial ya deja claro que hay derechos que no la requieren. En este sentido, sirva como ejemplo la ya citada sentencia del Tribunal Supremo 489/2018, de 23 de octubre, que cita en su fundamento de derecho cuarto, varios ejemplos en los que esa intervención judicial no es necesaria cuando se trata de limitar derechos fundamentales[129].

[127] En la Circular de la Fiscalía General del Estado 1/2019, de 6 de marzo, expresamente se afirma que «*la referencia expresa a la jurisprudencia, tanto del Tribunal Supremo como del Tribunal Constitucional que hace el preámbulo, debe interpretarse como la voluntad legislativa deliberada de integrarla en el texto legal mediante incorporación expresa o, en cualquier caso, como guía interpretativa de las nuevas disposiciones*». Pág. 3

[128] Así lo pone de manifiesto el propio legislador y varios autores. Vid CONDE PUMPIDO TOURÓN, Cándido. *La reforma procesal. Registro de sistemas informáticos, ampliación del registro a otros sistemas. El registro remoto de dispositivos informáticos (arts. 588 sexies y 588 septies LECRIM)*. Ponencia presentada en las Jornadas de formación organizadas por la Fiscalía General del Estado con fecha 10 de marzo de 2016 en materia de criminalidad informática. https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20Conde-Pumpido%20Tourón.pdf?idFile=4d9fe168-e9ee-4cd9-a783-68eab6158e47. Pág. 3, y páginas 6 y siguientes sobre la jurisprudencia que aborda algunas diligencias.

[129] La sentencia cita algunas sentencias del Tribunal Supremo que se refieren a casos en los que se producen cacheos, exploraciones radiológicas, detenciones, etc. Todos ellos se presentan como situaciones en las que los derechos que se

No obstante, la nueva regulación procesal exige que todas las diligencias de investigación electrónica, con independencia del derecho concreto del art. 18 CE que se vea afectado, sea ordenada, previa y preceptiva valoración, por un Juez.

Esta intervención judicial viene exigida en la actualidad por mandato legal, y toma como punto de partida y fundamento el derecho al propio entorno virtual del que más extensamente se habló en un apartado anterior, y al que hay que remitirse. Lo relevante de la nueva regulación es que la decisión sobre la limitación de los derechos del art. 18 CE que se pudiera producir como consecuencia de una diligencia de investigación en el ámbito de dispositivos electrónicos es atribuida al Juez, si bien, en algunos casos muy concretos, se admite, por razones de urgencia, que la medida se adopte por la policía o por el Ministerio Fiscal y se someta a posterior ratificación judicial, siempre en muy escaso lapso temporal.

(ii) Que el contenido de la resolución que accede a la práctica de la intervención solicitada esté sujeta a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad.

El contenido de cada uno de estos principios está definido en el texto legal y se analizan justo a continuación. Puede decirse que se trata de un conjunto de principios rectores de necesaria concurrencia. Es decir, se trata de criterios que, de ser apreciados en el supuesto sometido a decisión, determina y justifica la procedencia de la adopción de la diligencia. Se pretende por el legislador que la decisión se motive y justifique, reforzándose de este modo la seguridad jurídica de su adopción. Muy resumidamente, y sin perjuicio del desarrollo de cada uno de ellos, puede decirse que todos esos principios van dirigidos a comparar la situación que se presenta al Juez, junto con el tipo penal que presuntamente puede estar cometiéndose a juicio de los investigadores, con el derecho que puede limitarse de acordarse la diligencia. El legislador atribuye al Juez esa labor comparativa y valorativa.

(iii) Respeto debido a algunas exigencias formales. Principalmente tales requisitos se resumen en la necesidad de que la diligencia sea solicitada mediante escrito, que tendrá un contenido informativo mínimo imprescindible y que también debe ser respondido en un tiempo concreto, previo informe del Ministerio Fiscal.

---

limitan en cada caso ceden ante la necesidad de salvaguardar otros intereses superiores, y esta limitación no es decidida por un Juez, sino que se determina por parte de los agentes de policía, en el cumplimiento de sus funciones.

La existencia de presupuestos formales a la hora de acordar una diligencia de investigación electrónica constituye también una novedad de la reforma. Estos requisitos se aprecian tanto en el oficio de solicitud de la diligencia, como en el contenido mínimo de la resolución judicial que estime o rechace la petición. También hay exigencias formales al declarar el secreto de la medida adoptada, así como sus prórrogas, al control de su realización, y a la afectación a terceros de la medida y los usos de estos datos obtenidos en otros procedimientos. Por otro lado, hay concretas diligencias que además de los presupuestos generales, deben cumplir con otras exigencias que les son propias. En general en esos casos lo que se hace es reforzar el deber de información mínima que debe contener el oficio, o bien se restringe el ámbito de investigación a los que dichas diligencias se pueden aplicar, etc. En este trabajo se estudiará una de ellas, concretamente la diligencia de registro remoto de equipos informáticos, que es una de las diligencias que presenta un reforzamiento de presupuestos para su adopción.

Una vez sentados las características esenciales de los principios de general aplicación a las diligencias de investigación, lo que procede a continuación es analizar el contenido de cada uno de los principios rectores que se recogen en el texto legal.

2.2. Principio de especialidad.

El principio de especialidad del art 588 bis a), apartado 2 de la LECrim, exige que una medida de intervención en los derechos constitucionales de un ciudadano esté relacionada con la investigación de un delito concreto y determinado[130]. Dice el precepto que «*No podrán autorizarse medidas de investigación tecnológica que tengan por objeto prevenir o descubrir delitos o despejar sospechas sin base objetiva*».

El contenido de este primer principio rector exige que la medida limitadora de derechos que se solicita al Juez Instructor, por parte de los agentes investigadores, esté relacionada con la persecución de un delito concreto, con una investigación determinada, con un hecho que está siendo seguido e investigado por parte de los Cuerpos y Fuerzas de seguridad del Estado en esos momentos. Con la inclusión de esta exigencia, se pretende evitar que se usen las medidas de intervención en los derechos del art. 18 CE como un método indiscriminado de averiguación de

[130] Ver Circular de la Fiscalía General del Estado 1/2019, de 6 de marzo. Pág. 3

todo tipo de delitos, que no estén siendo investigados previamente, y como una forma genérica de investigación.

Siendo más preciso, resulta prohibido usar estas diligencias para reunir datos sobre la actividad de una persona, de la que previamente no existe sospecha o evidencia de que haya cometido un delito, o existiendo esa sospecha, no estén, al menos, algo acreditadas por otros medios de investigación que no sean el uso de esta clase de diligencias.

Por lo tanto, no podrán acordarse medidas de investigación de esta naturaleza en el ámbito de unas diligencias indeterminadas. Solo podrán acordarse dentro del ámbito de unas diligencias previas, de un sumario o de cualquier otro procedimiento de investigación concreto de los comprendidos en las normas procesales [131], que hayan sido aperturadas precisamente para investigar unos hechos indiciariamente expuestos y acreditados de forma sencilla. De manera que, siempre es necesario que exista una previa investigación formal abierta para poder adoptar cualquiera de estas diligencias de investigación tecnológicas.

La Sala II del TS sobre esta exigencia impuesta por el principio de especialidad ha puesto de relieve que la resolución que *«determine la adopción de la medida deberá precisar el delito cuya intervención lo hace necesario, en orden a (....) la evitación de "rastreos" indiscriminados de carácter meramente preventivo y aleatorio sin base fáctico previa de la comisión de delito, absolutamente prescrita en nuestro ordenamiento»*[132]. En suma, se exige, insoslayablemente, que el delito pueda intuirse, que exista alguna evidencia del mismo, y a posteriori, si ello es necesario, y concurren las demás condiciones junto con esta, se acuerde la adopción de la medida limitativa de derechos fundamentales que se solicite.

El principio de especialidad es uno de los presupuestos auténticamente esenciales en el ámbito de las intervenciones de comunicaciones y datos y, tras la entrada en vigor de la reforma de la LECrim, también de las diligencias de intervención de dispositivos de almacenamiento masivo de datos y de intervención remota de equipos.

No se trata de un principio aislado, sin conexión alguna con aspectos netamente prácticos en la adopción de la medida. Muy al contrario, de su estudio se han derivado doctrinas muy relevantes y de tremenda actualidad y aplicación en el ámbito de la investigación y la instrucción de delitos, como puede apreciarse con la simple lectura de la jurisprudencia [133].

---

[131] STS 878/2016, de 22 de noviembre. Ponente: Don Andrés Palomo del Arco.
[132] STS 60/2012, de 8 de febrero. Ponente: D. Juan Ramón Berdugo Gómez de la Torre, que cita a su vez la STS 999/2004, de 19 de septiembre.
[133] STS 71/2007, de 8 de febrero. Ponente: D. Juan Ramón Berdugo Gómez de la Torre. La citada sentencia, en su fundamento jurídico segundo, tras realizar un estudio del contenido del principio de especialidad, pone el mismo en

2.3. Principio de idoneidad.

El segundo principio que se recoge en la enumeración del art. 588 bis a, apartado 3 LECrim, es el principio de idoneidad. Se define textualmente como el que «*servirá para definir el ámbito objetivo y subjetivo y la duración de la medida en virtud de su utilidad».*

El criterio de la idoneidad es empleado por el legislador, y ya antes por la jurisprudencia que lo desarrolló, como un método o una pauta de control. Se trata de un principio que acentúa mucho tres aspectos concretos: el temporal, el objetivo referente a los hechos, y el que guarda relación con el propio investigado o subjetivo.

El principio de idoneidad sirve como regla para determinar si la medida solicitada, puesta en relación con los hechos que se investigan, es la más adecuada, y la que más se ajusta a los hechos que se exponen, y por consiguiente es apta para producir el resultado perseguido[134]. Por el contrario, la medida no será idónea si puede acudirse al empleo de vías de investigación distintas a las solicitadas, que no supongan la limitación, mas o menos intensa, de ningún derecho constitucional.

Pese a que la idoneidad no sea mas que un principio que sirve para valorar si lo solicitado por la fuerza policial actuante se adecúa a la entidad de los hechos, y conforme a ello puede producir el resultado previsto, se ha de analizar también si con su adopción se sirve al fin pretendido, atendido los distintos aspectos que se encuentran en juego, etc. Esta relación de progresión y adecuación viene siempre puesta en relación con el resultado que se espera obtener, es decir, si la *«medida es la adecuada para alcanzar la finalidad perseguida»* [135].

En muchos, casos este resultado sólo puede ser valorado a posteriori, es decir, tras haberse llevado a cabo, sobre todo si tras su práctica no se obtuvieron los resultados deseados cuando se acordó. Sin embargo, lo que se exige es un juicio de racionalidad acerca de si será posible obtener dichos resultados con los indicios mostrados por los investigadores.

---

relación con determinadas doctrinas, de relevante importancia práctica en el ámbito de la instrucción procesal penal y la investigación delictiva. De entre esas doctrinas podemos destacar la del "descubrimiento casual u ocasional" de notable importancia cuando durante la instrucción de un delito aparecen indicios de la comisión de otro distinto. Por otro lado, la resolución citada realiza una acertada definición del principio de especialidad cuando determina que «*El principio de especialidad exige que la decisión jurisdiccional de intervención de las comunicaciones telefónicas esté siempre relacionada con la investigación de un delito concreto, cuyos elementos ya se dibujan, al menos en el plano indiciario que permite el estado incipiente del proceso».*

[134] Circular de la Fiscalía General del Estado 1/2019, de 6 de marzo. Pág. 7

[135] Cfr. CASANOVA MARTÍ, Roser. *Las intervenciones telefónicas en el proceso penal*. J&B Bosch procesal. España. 2014. Pág. 224. El autor hace mención, a su vez, a varias sentencias dictadas por el Tribunal Supremo en las que se determina que la medida limitadora es considerada como una medida idónea porque de su práctica se pueden obtener resultados adecuados y útiles para la investigación.

En ese caso, una vez valorado, si a pesar de todo no se obtienen resultados satisfactorios en la práctica de la diligencia, no cabe la nulidad de la intervención. La diligencia practicada es válida y su ejecución, con independencia del resultado, descansa en el ejercicio de la motivación y ponderación realizada por parte del Juez instructor en su resolución. La resolución habilitante se confecciona atendiendo a una ponderación de la idoneidad de esa medida efectuada *ex ante*, no *ex post*.

El acto judicial de adopción de la medida requiere realizar un ejercicio de motivación suficiente, que permita conocer a cualquier persona las razones por las que la medida limitadora aparece como la más razonable y la más adecuada, puesto que la justificación de estas dos exigencias la convierte en idónea para el fin pretendido[136].

El legislador determina tres aspectos que conllevan que la medida sea idónea. La definición describe los aspectos objetivo, subjetivo y temporal[137]. El legislador no define a ninguno de los tres. En todo caso la medida interesada será considerada idónea si objetivamente es apta para obtener resultados[138], es decir, sirve para la finalidad para la que se adopta.

El criterio enumerado en primer lugar, el de carácter objetivo, admite que la idoneidad de la diligencia ha de ser puesta en relación con los hechos descritos en el oficio. Puede analizarse en el auto si los hechos que se describen en el oficio policial y su posible subsunción en la norma penal son objetivamente graves, y de suficiente entidad, como para acordarla, pero, sobre todo, si esos hechos pueden ser investigados de manera efectiva con la diligencia solicitada.

En segundo lugar, la ley alude a un criterio subjetivo que tampoco se define. De hecho, este criterio viene siendo considerado como una vía que sirve para modular la concesión o denegación de la diligencia de investigación limitadora de algún derecho del art. 18 CE. Este criterio subjetivo se refiere al conocimiento que los investigadores tengan de los sospechosos. Pueden y deben aportar sus antecedentes policiales, si es que fueran conocidos. Se trata de aportar información acerca de quiénes son los investigados desde un punto de vista criminalístico, de forma que adviertan de un alto grado de probabilidad de su participación en la comisión del delito investigado. Como aspecto

[136] STS 106/2017, de 21 de febrero. Ponente: Antonio del Moral. La sentencia considera que para superar el control de la legalidad de la intervención admitida *«no se trata de exigir una información exhaustiva de la policía, sino de comprobar si las informaciones que proporcionan representan "objetivamente" un sustrato que racionalmente hace pensar en la comisión de un delito, en la implicación en él de las personas cuyo derecho fundamental va s en afectado y en la idoneidad de una intervención de las comunicaciones para esclarecerlo».* Como puede apreciarse el propio Tribunal Supremo en este criterio ya está analizando aspectos subjetivos y objetivos que deben tenerse en consideración para legitimar la medida.

[137] Vid. MARCHENA GÓMEZ; GONZÁLEZ CUÉLLAR SERRANO, Op. Cit. Pág. 214.

[138] STS 85/2017, de 15 de febrero. Ponente: D. Joaquín Jiménez García. Se dice textualmente en el fundamento de derecho cuarto: «*En relación a la idoneidad porque este medio aparezca adecuado para los fines de la instrucción».*

subjetivo que también se puede tener en consideración no hay razón para descartar la información que se aporte sobre quiénes son las posibles víctimas.

En tercer lugar, el criterio referente al tiempo necesario para practicar la diligencia, es el que sirve para que en la resolución se valore la previsión respecto del tiempo que se deberá esperar para obtener un resultado o la urgencia que presenten los hechos; lo que se trata es de conjugar los datos aportados con un juicio de probabilidad relacionado con el tiempo necesario para obtener un resultado.

El criterio temporal puede ser relacionado con el subjetivo, de forma que se obtenga un juicio de probabilidad que sume la información tanto de las personas investigadas, con los hechos concretos y su gravedad, analizada bajo el prisma de su tipificación o de la alarma social que genera el asunto. Estos dos aspectos pueden determinar si la medida debe durar más o menos tiempo, o graduar la urgencia que requiere la investigación solicitada. La conjunción de estos aspectos deberá comportar un ejercicio de reflexión por parte del Juzgador expresada en la resolución que sirva para determinar si procede, en abstracto, conceder la medida solicitada.

Aplicando todo lo anterior al acceso y registro de un dispositivo de almacenamiento masivo de datos, debemos entender que la medida es idónea si permite encontrar en el interior del mismo una pluralidad de datos de diversa índole. Por lo demás estos aspectos objetivos, subjetivos y temporales pueden servir de criterios de orientación para fijar las pautas de búsqueda dentro del dispositivo.

Estos criterios son igualmente aplicables a la diligencia de registro remoto de equipos, pues asemejándose a una intervención de comunicaciones telefónicas, con mayor razón será necesario fijar la adecuación de la intervención solicitada a los hechos investigados y al autor (lo que es especialmente importante en los casos que hagan uso del aparato varios usuarios), y valorar de manera rigurosa si esta medida es la más apta para obtener la información que se necesita por los investigadores.

2.4. Principios de excepcionalidad y necesidad.

Los siguientes principios enumerados en el art. 588 bis a, apartado 4 de la LECrim, son dos: la excepcionalidad y la necesidad[139] de la medida de investigación. Ambos principios actúan como criterios moduladores y son de evaluación preceptiva por parte del juez. De forma que solo tras esa

[139] Circular de la Fiscalía General del Estado 1/2019, de 6 de marzo. Pág. 8

evaluación, debidamente expuesta, se ha de llegar a una conclusión que permita o deniegue la solicitud de intervención limitativa del derecho fundamental.

El legislador considera cumplimentada la observación correcta de estos principios cuando se dan dos situaciones que describe textualmente del siguiente modo:

«*a) no estén a disposición de la investigación, en atención a sus características, otras medidas menos gravosas para los derechos fundamentales del investigado o encausados igualmente útiles para el esclarecimiento del hecho, o,*

b) cuando el descubrimiento o la comprobación del hecho investigado, la determinación de su autor o autores, la averiguación de su paradero, o la localización de los efectos del delito se vea gravemente dificultada sin el recurso a esta medida».

Los dos apartados descritos evocan una situación en la que sólo acudiendo a la práctica de la diligencia interesada se podrá avanzar en la investigación. La excepcionalidad concurrirá cuando, al valorar los hechos, se llegue a la conclusión de que solo acudiendo a la medida solicitada se podrá investigar el hecho delictivo, su presunto autor, y el modo en que éste se ha llevado a la práctica, sin que exista ninguna otra manera para poder obtener un resultado[140]. Es un principio que descansa sobre la idea de que la limitación del derecho ha de ser lo menos frecuente posible, inusual, o la "ultima ratio", siendo siempre una medida a la que habrá de acudir de manera muy limitada[141] y de modo restringido.

Esta idea de excepcionalidad lleva a que sólo se permita la práctica de la diligencia solicitada cuando existan hechos constatados, con elementos e indicios suficientes y bajo circunstancias muy justificadas, pero que a la vez se concluya con que sólo con su realización se podrá obtener un resultado, o se esté ante situaciones apremiantes o necesarias. Por tanto, la excepcionalidad impone que solo en circunstancias que apreciadas en abstracto y comparando los dos derechos entre sí hará que ceda el derecho afectado por la diligencia.

Este principio ha de integrarse con el acatamiento del resto de principios[142], pero sin perder de vista que las diligencias limitativas de derechos ha de ser un recurso limitado, extremo y de aplicación

[140] STS 446/2004, de 19 de enero de 2005. Ponente: D. Andrés Martínez Arrieta.

[141] Este mismo aspecto ha quedado puesto de manifiesto incluso para los organismos encargados de ejercitar la acusación pública. Así lo exige la Circular de la Fiscalía General del Estado 1/2013, «Sobre pautas en relación a la diligencia de intervención de comunicaciones telefónicas». Pág. 73.

[142] SSTS 982/2016, de 11 de enero de 2017 y 993/2016, de 12 de enero de 2017. Ponente en ambas: D. Joaquín Jiménez García. Las dos sentencias contienen la misma definición del principio de excepcionalidad, resaltando su carácter limitado, manifestando que : «*De la nota de excepcionalidad se deriva que la intervención telefónica no supone un medio normal de investigación, sino excepcional en la medida que supone el sacrificio de un derecho fundamental de la persona, por lo que su uso debe efectuarse con carácter limitado, ello supone que ni es tolerable la petición sistemática en sede judicial de tal autorización, ni menos se debe conceder de forma rutinaria. Ciertamente en la mayoría de los supuestos de petición se estará en los umbrales de la investigación judicial --normalmente tal petición será la cabeza*

restringida, al que sólo cabe acudir cuando no exista otra forma de investigar los hechos[143]. Se trata de una idea que preside la redacción de todo el capítulo, y se aprecia en aspectos tales como: la duración limitada de la intervención (art. 588 bis e LECrim), o su prórroga (art. 588 bis f LECrim).

La excepcionalidad también ha de apreciarse en la actividad investigadora de los agentes[144]. Para ello el Juez Instructor tiene que valorar, a la hora de acordar o denegar la intervención solicitada, las previas actividades de investigación ya efectuadas. No es lo mismo haber realizado actuaciones de investigación previas antes de solicitar al Juez la correspondiente diligencia restrictiva de derechos fundamentales, que no haberlo hecho. Si, por ejemplo, consta en el oficio policial que se han realizado diligencias, como el seguimiento del presunto autor, haber analizado sus bienes, sus lugares de ocio habitual, las personas con las que se reúne, para llegar a unas conclusiones que se exponen al Juez Instructor, es más sencillo concluir que no se pueden efectuar más diligencias de investigación que aquéllas que son objeto de la solicitud. Si se pretende solicitar una diligencia limitativa de derechos habrá de acreditarse ante el Instructor que se han agotado otras vías menos lesivas para evitar limitar algún derecho, y que, pese a ello, no queda otra opción que limitarlo.

El segundo principio que acompaña al de excepcionalidad es el de necesidad. El término, por sí mismo, evoca la inevitabilidad limitadora del derecho en aras a la protección de otros derechos e intereses[145]. Una medida se considera necesaria cuando no pueda prescindirse de ella. Siguiendo el mismo silogismo, será innecesaria si hay otra medida, que no limite, en palabras del art. 588 bis a, apartado 4 LECrim, "*los derechos fundamentales del investigado*", que pueda ser adoptada y pueda preverse que permita obtener un resultado más o menos similar.

El citado precepto de la LECrim aporta como criterio que sirve para apreciar la necesidad, el hecho de que, en el caso de no usar la medida de investigación restrictiva del derecho fundamental, se pueda malograr o incluso se vea "gravemente dificultado" el conocimiento de los hechos investigados.

---

de las correspondientes diligencias previas--, pero en todo caso debe acreditarse una previa y suficiente investigación policial que para avanzar necesita, por las dificultades del caso, de la intervención telefónica, por ello la nota de la excepcionalidad, se completa con las de idoneidad y necesidad y subsidiariedad formando un todo inseparable, que actúa como valladar ante el riesgo de expansión que suele tener todo lo excepcional , riesgo sobre el que esta Sala ha llamado la atención varias veces. SSTS 998/2002 ; 498/2003 ; 182/2004 y 1130/2009».

[143] STS 233/2008, de 5 de mayo. Ponente: Don Manuel Marchena Gómez.

[144] STS 1119/2009, de 6 de noviembre. Ponente: Don Alberto Gumersindo Jorge Barreiro, o la STS 642/2007, de 6 de julio. Ponente: Don Manuel Marchena Gómez, que llega incluso a considerar como trabajo previo efectuado por los investigadores, el conocimiento que estos tienen de la habitual participación de los entonces imputados (ahora denominados investigados) en hechos de naturaleza criminal relacionada con el tráfico de drogas.

[145] El art. 8. 2. del Convenio para la protección de los derechos humanos y las libertades fundamentales aprobado en Roma en 1950 (publicado en el BOE de 6 de mayo de 1999), establece en relación con el derecho a respeto a la intimidad y al secreto de la correspondencia que «*no podrá haber injerencia en este derecho, sino en tanto que esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad pública, el bienestar económico del país, la defensa del orden ya la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y de las libertades de los demás*».

La excepcionalidad y la necesidad son dos principios muy relacionados entre sí. Ambos son una manifestación de que la diligencia limitadora debe considerarse como una opción límite, inusual y restringida. El juez instructor está obligado a valorar si sólo acudiendo a la medida de intervención solicitada, será posible investigar el delito, obtener información, encontrar al responsable o proteger a la víctima, y si no existe otro modo de hacerlo más que acudiendo a esta vía. Si el Juez Instructor concluye que así es, será una medida necesaria [146].

La jurisprudencia estima que hay necesidad cuando la medida de intervención es objetivamente hábil, y por lo tanto idónea, para obtener resultados positivos[147], y también cuando no existe más opción que la de seguir por dicha vía limitadora de derechos, al haber agotado todos los resortes de investigación mediante la práctica de otras diligencias menos invasivas y atentatorias a los derechos, tales como seguimientos personales, observaciones y vigilancias.

La llamada subsidiariedad, nombre con que en ocasiones ha denominado la jurisprudencia el principio de excepcionalidad, supone una exigencia conforme a la cual no ha de ser posible llevar a cabo las investigaciones por medios menos gravosos para la indemnidad de los derechos fundamentales que acudiendo a las medidas limitativas que constituyan el objeto de la injerencia judicial solicitada.

Estos dos principios, aplicados a las diligencias de acceso y registro a los datos de un dispositivo, concurrirán si los agentes acreditan que sólo ejecutándola se puede obtener un resultado satisfactorio y útil para la investigación. La función del Instructor será cerciorarse de ello, valorando la situación del procedimiento, si caben otros medios menos lesivos para los derechos del investigado con los que poder continuar con la investigación, etc. Teniendo presente que la operación valorativa ha de partir de la información que obre en el oficio policial, lo recomendable es que en la solicitud de la medida, la policía judicial, no escatime las explicaciones que sean necesarias sobre las diligencias que se han llevado a cabo hasta ese instante, para investigar los hechos, y se acompañe una exposición detallada sobre las razones por las que es necesario acudir a la diligencia de investigación concreta solicitada; que no se olvide, es mucho más limitativa en los derechos fundamentales que las ya realizadas hasta ese momento.

En esa labor el contenido del art. 588 bis, b) LECrim es muy útil, porque aporta un listado de materias y cuestiones que deben contenerse en el oficio policial de solicitud de la medida. El apartado 2º del párrafo 2 exige *"la exposición detallada de las razones que justifiquen la necesidad de la medida de acuerdo a los principios rectores establecidos en el art. 588 bis a)m, así como los*

[146] Vid. RIVES SEVA, Antonio Pablo. *La intervención de las comunicaciones en el proceso penal. Análisis doctrinal, legislación y jurisprudencia*. Bosch. Barcelona. 2010. Página 185.
[147] STS 751/2012, de 28 de septiembre. Ponente: Don Manuel Marchena Gómez.

indicios de criminalidad que se hayan puesto de manifiesto durante la investigación previa a la solicitud de autorización del acto de injerencia". El resto del precepto es una enumeración de la información a aportar al instructor.

El tenor del precepto exige que los agentes encargados de la investigación criminal aporten "*indicios de criminalidad"*, y no pruebas de la misma. Esto comporta para el Juez de Instrucción el necesario examen de dos requisitos: el primero exige analizar la concurrencia de un trabajo previo y suficiente por parte de los investigadores, del que pueda colegirse que la medida de intervención interesada es la única que les permitiría continuar con la investigación ya comenzada. Por otro lado, en segundo lugar, no se exige que el resultado de este trabajo sea absolutamente concluyente y seguro, pues de lo contrario se estaría exigiendo un verdadero principio de prueba, que no es exigido por el legislador[148], pero al menos permita considerar la existencia de hechos ilícitos que deben seguir siendo investigados.

2.5. Principio de proporcionalidad.

El párrafo 5 del art. 588 bis a) LECrim, regula el principio de proporcionalidad[149]. Lo más característico de este principio es que parece ser de aplicación prioritaria a todos los demás, y se puede considerar, a su vez, como el resultado de la suma de todos los principios anteriores, pero sin requerir la plena exigencia de todos ellos. Puede tratarse como un principio resumen de los demás, si bien, goza de autonomía cuando lo apreciamos apegado a la concreta entidad de los hechos que son objeto de investigación, y puesto en relación con la medida que se pide.

---

[148] STS 358/2017, de 18 de mayo. Ponente: Don Carlos Granados Pérez. La sentencia establece que dentro de dicho principio de aportación de datos al órgano instructor, estos han de ser suficientes para configurar "sospechas fundadas" que deben estar «*basadas en alguna clase de datos objetivos, que han de serlo en un doble sentido: en el de ser accesibles a terceros, sin lo que no serían susceptibles de control; y en el de que han de proporcionar una base real de la que pueda inferirse que se ha cometido o que se va a cometer el delito, sin que puedan consistir en valoraciones acerca de la persona. Han de excluirse las investigaciones meramente prospectivas, pues el secreto de las comunicaciones no puede ser desvelado para satisfacer la necesidad genérica de prevenir o descubrir delitos o para despejar las sospechas sin base objetiva que surjan de los encargados de la investigación, ya que de otro modo se desvanecería la garantía constitucional; exclusión que se extiende igualmente a las hipótesis subjetivas y a las meras suposiciones y conjeturas, pues si el secreto pudiera alzarse sobre la base de esas hipótesis, quedaría materialmente vacío de contenido (SSTC49/1999; 166/1999; 171/1999; 299/2000; 14/2001; 138/2001; 202/2001; 167/2002; 261/2005; 136/2006;253/2006; 148/2009; 197/2009; 5/2010; y 26/2010*)».

[149] 588 bis a), 5. «*Las medidas de investigación reguladas en este capítulo sólo se reputarán proporcionadas cuando, tomadas en consideración todas las circunstancias del caso, el sacrificio de los derechos e intereses afectados no sea superior al beneficio que de su adopción resulte para el interés público y de terceros. Para la ponderación de los intereses en conflicto, la valoración del interés público se basará en la gravedad del hecho, su trascendencia social o el ámbito tecnológico de la producción, la intensidad de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho».*

Los principios legales que se han visto hasta ahora son dotados por el legislador y por la jurisprudencia de una autonomía y contenido propios, pero el principio de proporcionalidad puede ser entendido como un meta-principio o supra principio que integra a todos los demás, y al mismo tiempo permite, en base a los hechos que se presentan, como la principal justificación para la adopción de la medida limitadora de derechos fundamentales que en cada caso se solicite. Es el principio de mayor preponderancia en la medida en que se apega a los hechos, a su entidad, relevancia, gravedad e importancia, y con su mera concurrencia admite la adopción de la diligencia.

La redacción dada por el legislador al artículo alude a la gravedad del hecho, a diversas circunstancias presentes en el caso, a la entidad que los hechos investigados puedan presentar en relación con el derecho que se pretende limitar, etc. La suma de estas variables, sin tener en cuenta ningún otro aspecto que el que va más allá de los hechos, es el que permite concluir con su mayor importancia, en consonancia con la consolidada jurisprudencia constitucional referida a la limitación o restricción de los derechos fundamentales.

La medida de intervención en los derechos individuales puede considerarse como una medida proporcionada, con carácter general, cuando es solicitada para investigar un delito concreto, que ya esté siendo objeto de investigación (principio de especialidad); cuando objetivamente puede servir para averiguar el hecho cometido o qué aspecto desconocido se pretende determinar: autor o autores, partícipes, etc. Se entenderá proporcionada la medida cuando además se trate de una diligencia insustituible, es decir, que no exista otro método menos invasivo en los derechos fundamentales del investigado que aquél que ha sido solicitado. En último lugar, la proporcionalidad se apreciará también, si sólo con esa diligencia se está ante el único medio adecuado para averiguar el hecho, o algunas de sus circunstancias, pese a haber efectuado otras diligencias. En todo caso, además de estos aspectos, lo fundamental para la concurrencia de la proporcionalidad, es que hay que poner en relación la gravedad del hecho investigado con el derecho que se pretende limitar, porque en ese análisis de comparación, si la gravedad de los hechos resulta evidente, la proporcionalidad de la medida estará justificada, pese a que los demás aspectos no estén tan presentes.

Es un principio cuya relevancia y preminencia permite, con su mera concurrencia admitir la limitación del derecho constitucional afectado. Esto es, cabe la posibilidad de acordar diligencias que limiten derechos fundamentales sin tener justificados los demás principios, pero ante la gravedad del hecho su ejecución se aprecia como una medida adecuada. Esta urgencia, que se deriva de la comparación entre los hechos acontecidos y los derechos constitucionales afectados hace que deban ceder los segundos para evitar mayores perjuicios. Cuando esto concurre, lo hace la

proporcionalidad de la medida, de ahí que se pueda aseverar que el principio de proporcionalidad es un verdadero meta-principio.

La medida es proporcional cuando tras una operación valorativa efectuada en conjunto se obtiene como resultado su necesidad insoslayable. Es evidente que llevarla a cabo con la concurrencia de todos los demás principios y presupuestos ya enumerados es lo preferible, pero no es necesario que todos concurran con la misma intensidad, ya que lo fundamental es que el acto de comparación del beneficio que proporcionaría la medida en relación con la limitación del derecho constitucional implicado debe conllevar adoptar la medida[150]. Todos los principios han de ser debidamente ponderados entre sí. El juez en su resolución, debidamente motivada, tendrá que expresar qué principios son los que considera concurrentes, pero en todo caso la proporcionalidad alude a la relación que hay entre el hecho que es objeto de investigación y la necesidad de tener que realizar cualquier diligencia que limite derechos constitucionales, y cómo se impone la necesidad expresada en segundo lugar, atendida principalmente la situación (que no es más que la suma del hecho, del tipo de delito, de los indicios que se aportan y de la identidad del sujeto)[151].

En todo caso, lo óptimo es que concurran todos los principios, pues esto hace que la diligencia resulte proporcionada. En este sentido, lo que la doctrina exige es la concurrencia de *«juicio previo de ponderación de bienes en conflicto…necesidad de la medida y..que la medida sea ponderada y equilibrada»* [152]. La prevalencia de la ponderación de circunstancias en conflicto es lo relevante para la concurrencia de este principio, y en el desarrollo de ese juicio valorativo no siempre es necesaria la concurrencia de los demás aspectos que introducen los otros principios rectores, pues

---

[150] Vid. PERELLO DOMENECH, Isabel. «El principio de proporcionalidad y la jurisprudencia constitucional». *Revista Jueces para la Democracia*. Nº 28. 1997. Págs. 69 a 75.

[151] En la STS 689/2016 de 27 de julio. Ponente: Don Pablo Llarena Conde, se dice textualmente que *«En todo caso, el juicio de pertinencia de la intervención no precisa de una motivación específica, individualizada y secuencial de cada uno de los presupuestos y principios que debe satisfacer la restricción del derecho, tal y como el recurso parece sustentar. El juicio de proporcionalidad implica una valoración sobre la gravedad del delito, sobre los indicios de su existencia y de la intervención del sospechoso, y sobre la necesidad de la medida, todo ello puesto en contraste con la importancia del derecho que pretende limitarse y la extensión temporal de su restricción; debiendo el Juez explicitar todos los elementos indispensables para realizar la ponderación y para hacer posible su control posterior (SSTC 299/2000, de 11 de diciembre; 167/2002, de 18 de septiembre). Nuestra recientemente aprobada reforma de la LECrim concreta en su artículo 588 bis A.5 que " Las medidas de investigación reguladas en este capítulo solo se reputarán proporcionadas cuando, tomadas en consideración todas las circunstancias del caso, el sacrificio de los derechos e intereses afectados no sea superior al beneficio que de su adopción resulte para el interés público y de terceros. Para la ponderación de los intereses en conflicto, la valoración del interés público se basará en la gravedad del hecho, su trascendencia social o el ámbito tecnológico de producción, la intensidad de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho».* En este sentido lo que puede destacarse es que el propio Tribunal da importancia a la conjunción de todos los aspectos esenciales que justifican la medida bajo el manto de la proporcionalidad, mucho más que al hecho de atender a la justificación separada y exhaustiva de cada uno de los principios esenciales por separado. Esta misma idea es sostenida en RODRÍGUEZ LAINZ, en su trabajo denominado. «Sobre la dimensión temporal de las medidas de investigación tecnológica». *Base Doctrinal Ed. SEPIN*. Nº DOCUMENTO SP/DOCT/75471. Mayo 2018. Pág. 3.

[152] Cfr. PERANDONES ALARCÓN, Marta. «La recíproca limitación de los derechos fundamentales y la averiguación de la verdad en el proceso penal». *La Ley Penal*, Nº 117, Noviembre-Diciembre 2015. LA LEY 7547-2015. Pág. 3. .

en no pocas ocasiones la valoración viene condicionada por la gravedad de los hechos que se presentan, y su comparación con los derechos a limitar. El tenor literal del art 588 bis a, 5 de la LECrim, que es el que introduce en el texto legal este principio, es muy similar al contenido del art. 8.2 del Convenio para la protección de los derechos humanos y las libertades fundamentales aprobado en Roma en 1950. Son dos preceptos que se complementan[153]. El Convenio fue incorporada al derecho interno, conforme a la previsión contenida en el art. 96.1 de la Constitución, mediante su publicación en el Boletín Oficial del Estado de 6 de mayo de 1999, con lo que adquirió plena vigencia y exigibilidad jurídica en nuestro Derecho.

El art. 8.2 del Convenio recoge distintas situaciones en las que se estima necesario y justificado la limitación del derecho a la intimidad y la preservación del secreto de la correspondencia postal (lo que evidentemente será también extensible a los dispositivos que, en sus versiones actuales, son susceptibles de contener los datos y elementos cuya intangibilidad en su comunicación es protegida por estos derechos). En este sentido, debe ponerse de relieve que el Convenio contiene unos criterios más amplios que los previstos en la LECrim a la hora de regular las eventuales limitaciones de los derechos fundamentales vinculados con el secreto de las comunicaciones y con el derecho a la intimidad. De manera que, teniendo en cuenta que estos criterios del Convenio son derecho interno, es posible sostener que justifican la exigencia de elementos adicionales, que avalen la proporcionalidad de la medida limitadora de derechos fundamentales.

Entre los criterios más importantes que se citan por parte del Convenio y que sirven a su juicio para justificar una posible limitación de derechos constitucionales está la necesidad de prevenir delitos (lo que admite la exigencia del principio de especialidad tanto del delito que esté siendo objeto de análisis e investigación previos, como de la persona concreta y determinada sobre la que ya habrá debido existir alguna clase de investigación), asegurar la protección de la salud o la de proteger los derechos y las libertades de los demás. Los criterios que aporta el Convenio exigen la valoración de la gravedad de un hecho, y justifican, en caso de que concurran la admisibilidad, adecuación y utilidad de la medida.

[153] Dice el artículo 8 del Convenio, bajo la rúbrica "Derecho al respeto a la vida privada y familiar", en su párrafo 1 que «*Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia*». Lo que se contiene en este primer párrafo es el reconocimiento de los derechos que ya han sido debido objeto de análisis en otras partes de este trabajo, y que se ciñen al derecho al secreto de las comunicaciones telefónicas, postales y de cualquier otro tipo, así como el derecho a la intimidad personal y familiar y el derecho a la inviolabilidad del domicilio. El párrafo segundo, que es el que interesa en este momento dice que: « *No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás*».

En este sentido la Circular de la Fiscalía General del Estado 1/2019[154] estima que los aspectos que inciden en el juicio proporcionalidad son la gravedad y entidad del hecho, la trascendencia o alarma social que genera[155] , la intensidad de los indicios aportados a las actuaciones, y la comparación entre el resultado que es perseguido y el derecho que se tiene que limitar para conseguirlo.

El principio de proporcionalidad se ha definido como el que pretende *«buscar el equilibrio ponderando los intereses en conflicto, esto es, el ius puniendi del Estado, por un lado y el ius libertatis del ciudadano por otro»* [156]. Es el principio que cumple con una función de equilibrio de intereses contrapuestos en el proceso penal, lo que permite volver a la idea de que se trata de un principio aglutinador de los demás, y un criterio preferente en caso de necesidad, pero siempre desde la perspectiva de los hechos que se presentan a valoración.

La proporcionalidad, además de un principio de valoración de la necesidad de una diligencia de investigación, es también un principio general del derecho, aplicable a todas las ramas jurídicas en las que sea necesario ponderar varios intereses en juego de forma que se tenga que decidir acerca de la adopción de una medida, atendidas todas las vicisitudes que pueden concurrir en un supuesto de hecho.

El que el legislador lo haya recogido en el último lugar de la enumeración de los principios aplicables a la intervención de cualquier clase de derecho, y más concretamente en nuestro caso, a la intervención de datos albergados en un dispositivo, no es una decisión arbitraria o caprichosa. Esta posición en la LECrim puede ser explicada y entendida si se atiende a este principio desde una posición que lo considera como un elemento resumen o aglutinador de todos los demás principios que se han analizado. Coadyuva a esta interpretación la propia dicción literal del art. 588 bis, apartado a, 5 LECrim, cuando exige tomar en consideración todas las circunstancias del caso. En este sentido, esta posición hermenéutica, última en aparecer y que supone una síntesis de las demás, permite invocar el principio de proporcionalidad ante circunstancias graves.

2.6. Principio de necesaria intervención judicial y de resolución motivada.

[154] Pág. 10 a 12.
[155] Para apreciar la concurrencia de alarma social, la Circular incide con particular énfasis en los casos que el delito se haya cometido instrumentos tecnológicos, en particular por el efecto expansivo que tiene la comisión de determinados delitos a través, por ejemplo, de las redes sociales.
[156] Cfr. NOYA FERREIRO, María Lourdes. «Presupuestos constitucionales de las medidas de intervención de las comunicaciones I». *Revista xuridica da Universidade de Santiago de Compostela*, Vol. 8, Nº 2, 1999. Págs. 151.

Los principios ya expuestos son los esenciales, y los que cuentan con una mención expresa en el texto legal. Pero junto a ello, hay elementos que a pesar de no estar expresamente enunciados como principios, han sido usualmente exigidos en la jurisprudencia relativa a la limitación de derechos fundamentales, y cuya necesidad también se deriva del texto legal. Pueden citarse dos de ellos:

(i) El principio de necesaria intervención judicial, uno de cuyos fundamentos se encuentra en la expresión *«previa autorización judicial»*[157] contenida en la LECrim.

(ii) El principio de necesaria resolución motivada, como modo de exteriorización de la decisión adoptada puede considerarse como otro de ellos.

Estos dos principios ya existían, y estaban plenamente vigentes, en la jurisprudencia anterior a la entrada en vigor de la LO 13/2015. La nueva redacción de la norma procesal penal no modifica su exigencia, pero no los considera como principios rectores. En todo caso, pese a no considerarse como principios rectores, como les sucede a los anteriormente estudiados, el tenor literal de la norma permite afirmar su exigencia y su vigencia, tratándose además de aspectos que se ven garantizados, reforzados, consolidados, ampliados y clarificados en la reforma de la LECrim[158]. El contenido del art. 588 bis c, párrafo primero exige expresamente auto motivado dictado por el Juez de Instrucción. Esta expresa mención fundamenta la inclusión en la LECrim de estos dos elementos, recogiendo así lo que hasta ese instante era una consolidada doctrina jurisprudencial. Se sigue de esta manera el mismo proceso de inclusión de doctrina jurisprudencial en la ley, tal y como sucedía con los principios rectores.

El reconocimiento de estas exigencias, y su ubicación en el texto legal junto a su mención en la exposición de motivos, permite considerar que el legislador eleva a la categoría de principio fundamental el que cualquier limitación de derechos fundamentales (como lo son en este caso los derecho a la intimidad y al secreto de las comunicaciones), con independencia de que las exigencias constitucionales lo requieran o no, serán decididos y ordenados por el Juez. La resolución que acuerde cualquier clase de limitación de uno de los derechos constitucionales afectados por estas diligencias de investigación se adoptará mediante el dictado de una resolución escrita, en la que se valoren las razones fácticas y jurídicas que fundamenten su adopción. Una decisión judicial adoptada de este modo permite conocer a cualquier persona los razonamientos empleados para

[157] Cfr. MUERZA ESPARZA, Julio. *Las reformas procesales penales de 2015. Nuevas medidas de agilización, de investigación y de fortalecimiento de garantías en la justicia penal.* Thomson Reuters Aranzadi, Navarra. 2015. Pág. 161. Nota 6.

[158] STS 271/2017, de 18 de abril. Ponente: Doña Ana María Ferrer García. La sentencia expresamente señala que: *«La decisión al respecto corresponde exclusivamente del poder judicial, concretamente, al Juez de Instrucción, a quien compete la ponderación de los intereses en juego, mediante un juicio acerca de la proporcionalidad y necesidad de la medida, el cual deberá expresarse en una resolución judicial motivada».*

justificar la restricción de un derecho fundamental con ocasión de la autorización de la medida de investigación, que permite además, que esa decisión sea controlada por la vía de los recursos [159].

La lectura del anteriormente mencionado art. 588 bis c, apartado 1, es una concreción de la exigencia, que desde el inicio del Capítulo IV ya se aprecia en el art. 588 bis, apartado a, 1 LECrim, que exige una *«autorización judicial»* para acordar cualquier medida que limite derechos del art. 18 CE, en los mismos términos que ya han sido apuntados más arriba. Estas alusiones convalidan la afirmación de que el principio de judicialización de las medidas limitativas de derechos fundamentales, son más que una simple exigencia formal, y se actúa así conforme se exige en los apartados 2 y 4 del art.18 de la CE[160].

En segundo lugar, la judicialización no es sólo una mera atribución competencial, sino que conlleva un refuerzo en la motivación de la resolución[161]; aspecto éste que se configura como uno de los rasgos distintivos en la reforma[162]. La motivación de la resolución judicial que acuerde la diligencia es una exigencia recogida expresamente en el texto legal en el art. 588 bis c, apartado 1 de la LECrim, aunque no se considera en la ley como un principio rector.

La inclusión en el contenido de los diferentes artículos que regulan cada concreta diligencia de investigación, de aspectos individuales sobre los que el auto se tiene que pronunciar, son prueba de que el legislador pretende que cada resolución sea única, concreta y vinculada a circunstancias y fundamentos propios. Además, el refuerzo en la operación de motivación viene exigida incluso desde la propia exposición de motivos de la ley, en cuyo apartado IV, ya se requiere *«resolución judicial habilitadora, donde el juez determinará la naturaleza y extensión de la medida»*. Esta

[159] Cfr. LADRÓN TABUENCA. Op. Cit. Págs. 2-3. Sobre este particular se dice expresamente que *« Siendo esto así con carácter general, en mayor medida si se trata de resoluciones que permitan una limitación o restricción en el libre ejercicio de un derecho fundamental (sentencia del Tribunal Constitucional 54/1996), pues sólo así será posible comprobar que se ha procedido a valorar y ponderar el derecho fundamental afectado en aplicación del principio de proporcionalidad, el fin legítimo que ha de perseguir la medida, y las condiciones en que se ha de practicar la misma y aportarse sus resultados al proceso, y con ello, permitir, a la vez, un adecuado ejercicio del derecho de defensa (sentencias del Tribunal Constitucional 299/2000, de 11 de diciembre, 205/2002, de 11 de noviembre). »*

[160] En relación a la aplicación de este principio de intervención judicial, no debe perderse de vista que, en las diligencias de acceso y registro de datos, y también en todas las demás, la intervención judicial es doble, pues dicha participación concurre en el momento de valorar la limitación del derecho afectado en cada caso, pero también concurre dicha participación en el seno mismo de un proceso penal, que per se, también es atribuido a los jueces y tribunales.

[161] El tipo de resolución debe ser un auto, así lo exige el art. 588 bis c LECrim. Se trata de un tipo de resolución que, conforme al art 245.1.a) de la Ley Orgánica del Poder Judicial que *«las resoluciones de los jueces y Tribunales que tengan carácter jurisdiccional se denominarán [....] b) autos, cuando decidan recursos contra providencias, cuestiones incidentales, presupuestos procesales, nulidad del procedimiento o cuando, a tenor de las leyes de enjuiciamiento deban de revestir esta forma*». Dispone a su vez el art. 248.2 del mismo texto legal que «*los autos serán siempre fundados y contendrán en párrafos separados y numerados los hechos y razonamientos jurídicos y, por último la parte dispositiva. Serán firmados por el Juez, Magistrado o Magistrados que los dicten».*

[162] STS 723/2018, de 23 de enero de 2019. Ponente: Doña Ana María Ferrer García. La sentencia repara en este refuerzo de la motivación, aduciendo que *«Ciertamente la regulación procesal incorporada por la LO 13/2015 ha introducido mayores exigencias de motivación en la adopción de medidas de esta índole ».*

exigencia está ubicada en el mismo párrafo que se dedica a relacionar los principios rectores, lo que la convierte, junto a la judicialización, en algo más que simples requisitos formales.

Las pautas de motivación vienen incluidas en el texto de la ley, exigiendo el análisis y la ponderación de los diferentes intereses en juego, y de los derechos que pueden verse limitados. Es decir, tal y como dice el art. 588 bis a, apartado 5, al regular el principio de proporcionalidad, motivación implica tomar *«en consideración todas las circunstancias del caso».* Esta evidente relación entre la motivación y la proporcionalidad, unidos a los demás aspectos que se han ido relacionando, permite relacionar el contenido de los principios rectores ya analizados con estos otros dos axiomas, que de esta manera pasan a ser más que simples exigencias formales.

Los elementos que deben valorarse por el Juez Instructor se enuncian en el art. 588 bis, apartado a, 5 LECrim. Estos son los distintos derechos afectados por la medida, los intereses en juego, la concreta utilidad para el interés de terceros que ofrece adoptar la medida, así como para el propio interés público, etc. También sirve razonar sobre aspectos como la gravedad, la trascendencia social del hecho, el ámbito tecnológico de producción, la intensidad de los indicios, o la relevancia del resultado que se persiga. Es decir, se ofrecen diferentes criterios que, al tiempo que permiten concluir con la proporcionalidad de la diligencia, sirven para exteriorizar el razonamiento que fundamenta la decisión que se adopte.

La enumeración de los distintos factores a tener en cuenta para obtener una resolución auténticamente motivada, es una de las novedades de la reforma. Además de la existencia de los principios rectores del art. 588 bis a LECrim, puede apreciarse en el art. 588 bis c, apartado 3 todo el contenido que debe contener el auto. Ese contenido en ocasiones es más que simple información, requiriéndose un acto de explicación y razonamiento. Por ejemplo, el apartado c del párrafo 2 del articulo cuando habla sobre la extensión y alcance de la medida relaciona este aspecto con los principios rectores, y por lo tanto requiere de un ejercicio de motivación. Lo mismo puede decirse con respecto al apartado g del mismo artículo, relacionado con la finalidad de la medida. La exigencia de motivación se lleva, en ocasiones, hasta materias sobre las que los jueces no están especialmente preparados[163] .

Las operaciones de razonamiento y motivación exigidas al Juez, cuentan como contrapartida, con la obligación de que el oficio policial que solicita la diligencia que limite el derecho[164], cuente con

[163] Así, por ejemplo en la diligencia de intervención remota de equipos, que se realiza mediante el empleo de mecanismos informáticos a los que el Juez resulta completamente ajeno, la LECrim le exige expresamente pronunciarse acerca de la forma en que se procederá al acceso y a la aprehensión de los datos.

[164] La STS 216/2018, de 8 de mayo. Ponente: don Vicente Magro Servet, usa como paradigma de esta labora motivadora expresiones tales como «*La clave está, pues, en la exigencia de motivación en la solicitud policial de*

información suficiente. El oficio es la petición escrita dirigida al Juez por parte de los investigadores en la que se solicita que se adopten una o varias de estas medidas. Es, en numerosas ocasiones, la primera toma de contacto de los investigadores con el Juez (aunque no es necesariamente el primer conocimiento del asunto), y por eso, lo que parece más lógico, es que esa petición explique detallada y pormenorizadamente todos los indicios, diligencias, razonamientos, hipótesis y líneas de investigación que maneja la policía judicial. Aportar estos datos al Juez es necesario para decidir sobre la concesión o no de la medida. Por eso, la motivación se erige como una exigencia esencial, que grava a todos los sujetos implicados en la limitación de un derecho fundamental, y que, por supuesto resulta predicable también en las dos diligencias de investigación tratadas en esta tesis.

En conclusión hay que resaltar la importancia de la judicialización y la motivación como criterios rectores, que están expresamente recogidos en la ley. Estos criterios, pese a no formar parte de los principios rectores, entroncan directamente con ellos, en la medida en que su observancia eleva la seguridad jurídica en la adopción de la diligencia, cumpliéndose así una de las finalidades perseguidas por el legislador en esta reforma.

3. Requisitos formales para acordar una diligencia de investigación electrónica.

El conjunto de razonamientos que el Juez exprese en el auto que acuerde o deniegue la diligencia de investigación concretada en el oficio policial, debe contener un examen de los principios ya analizados. Esta decisión judicial debe seguir un cauce formal inexorable que se erige, también, en garantía de respeto a los derechos fundamentales implicados y en garantía de legalidad. El correcto seguimiento de estos aspectos formales contribuye así a la válida adopción de esa decisión judicial.

El artículo 588 bis b LECrim y el art. 588 bis c LECrim regulan los presupuestos y aspectos formales que deben concurrir para la válida intervención en cualquiera de los derechos fundamentales del art. 18 CE, si bien hasta antes de la entrada en vigor de la Ley Orgánica 13/2005 fue la jurisprudencia del Tribunal Supremo y del Tribunal Constitucional las que configuraron estos requisitos, así como el contenido mínimo que debía exigirse para que se produjera una limitación de los derechos del art. 18 CE.

---

intervención telefónica». Se trata de una de las primeras sentencias del TS que analiza la labor motivadora tras la reforma de la Ley Orgánica 13/2015.

Los requisitos formales para la adopción de una diligencia han dejado de estar vinculados a la doctrina jurisprudencial, que había sido la que configuraba un válido proceso de intervención[165], y han pasado a estar positivizados en el contenido de las normas jurídicas. Estos requisitos, en la actualidad, se refieren a las personas legitimadas para solicitar la intervención, cuáles son las exigencias mínimas que la solicitud debe contener, y cuál es el contenido mínimo que la resolución judicial debe reunir. También se deben incluir bajo este apartado las cuestiones relativas a la audiencia del Ministerio Fiscal, plazos de ejecución y renovación de la medida así como las exigencias derivadas de diferentes acontecimientos que se pueden producir durante la instrucción, como es el caso de los hallazgos casuales.

3.1. Solicitud: sujetos legitimados y forma de llevarla a cabo.

La limitación de un derecho fundamental mediante la práctica de una diligencia de investigación electrónica comienza por la petición al Juez de que ésta se lleve a cabo. Por ello, lo primero a discernir, será quiénes pueden solicitar que se practiquen alguna de estas medidas. La norma, en su texto, es muy clara sobre esto, y fija que la solicitud de limitación de un derecho del art. 18 CE puede provenir tanto de la Policía Judicial como del Ministerio Fiscal. La LECrim no niega ni admite que puedan solicitarlas las demás partes del proceso, pero es evidente de que caso de que así se hiciera no están obligadas a cumplir con las fuertes exigencias de contenido que se contienen en la ley, y que se dirigen a los solicitantes ya expresados. Habrá ocasión de ver, más adelante, que hay legislaciones en las que son las partes las que piden las diligencias.

En todo caso, habiendo de ceñirse a las exigencias que se imponen a estos dos solicitantes, deben ajustar su petición, al concreto contenido del apartado 2 del art. 588 bis b LECrim. Los diferentes ordinales de dicho apartado son los que detallan los requisitos de contenido mínimo exigibles para la solicitud de la diligencia. Se trata de exigencias bastante lógicas, y se resumen, en la aportación de toda la información que sea posible y que permita al Juez instructor, encargado de decidir sobre ella, formarse una opinión fundada sobre los hechos. Esta exigencia de información debe ser puesta en relación con el contenido que deberá tener el auto que decida sobre ello. Como la resolución

[165] Vid. MAGRO SERVET, Vicente. «Aspectos prácticos de la ejecución de las diligencia de investigación policial de intervención telefónica y de entrada y registro». *La Ley Penal*, Nº 65, Noviembre 2009, pág. 5. LA LEY 19958/2009. El autor, tras solicitar una expresa y profunda reforma legal que regulase las intervenciones, hace alusión a las SSTS de 17 de marzo de 2009, 6 de marzo de 2009 y 11 de febrero de 2009. La segunda de las sentencias citadas analiza cuál debe ser el contenido que debe de exigirse a un oficio policial que interese una medida de intervención de comunicaciones. Esto ejemplifica lo que se dice en el texto al afirmar que ha sido la doctrina jurisprudencial la que venía determinado las exigencias de contenido mínimo imprescindible en el oficio policial, para acordar una diligencia.

judicial debe contener necesariamente una serie de pronunciamientos y de valoraciones, la información que se suministre habrá de ser suficiente para que el contenido preceptivo del auto no falte.

La información que los solicitantes deben aportar necesariamente se enumera en los ocho apartados del párrafo segundo del art. 588 bis 2. Estos apartados se refieren a lo siguiente:

(i) En primer lugar, el apartado exige que se describan las circunstancias objetivas del hecho investigado, lo que alude a extremos tales como cuándo han sucedido estos hechos, dónde, qué ilícito penal podría estar siendo cometido, entre otros aspectos. Igualmente, se solicitan datos subjetivos, referidos a la necesidad de identificar al sujeto o sujetos que realizan activamente el tipo penal investigado, así como también a los afectados por la medida que limita el derecho del art. 18 CE que se limita. En lo que se refiere al sujeto, además de sus datos, se pueden aportar sus antecedentes policiales -no se suministran los antecedentes penales, pues los investigadores no tienen acceso a esa información que depende del Ministerio de Justicia [166] - o información sobre las detenciones que pudiera haber tenido por hechos similares [167]. En relación con los terceros afectados habrá ocasión de volver sobre su regulación. La ley admite que no se aporten estos datos, si no son conocidos por los agentes, y dejar dicha identificación para que sea precisamente uno de los aspectos que pueden derivarse de la práctica de la diligencia.

   En todo caso, además del resto de apartados que a continuación se analizan, sigue vigente la doctrina jurisprudencial que, sobre estos particulares, venía rigiendo antes de la reforma de la LECrim. Esta jurisprudencia venía exigiendo la aportación de información descriptiva suficiente tanto del hecho como del autor, así los indicios que permitan considerar la existencia racional de un hecho delictivo[168], e incluso se centraba en aspectos derivados de la obtención de dichos indicios [169].

[166] A meros efectos informativos el Registro Central de Penados se encuentra regulado en el Real Decreto 95/2009, de 6 de febrero, por el que se regula el Sistema de registros administrativos de apoyo a la Administración de Justicia. Por el contrario los antecedentes policiales sí que están a disposición de las Fuerzas y Cuerpos de Seguridad del Estado en tanto que éstos dependen del Ministerio del Interior, lo mismo que los archivos en los que se recogen esos antecedentes.
[167] Con la aportación de este tipo de información lo que se debe perseguir es la aportación de datos que permitan valorar la presencia del investigado en delitos de igual o parecida naturaleza en los que haya estado implicado en otros tiempos, etc
[168] STS 176/2015, de 25 de marzo. Ponente: Don Francisco Monterde Ferrer. La sentencia recoge en su fundamento de derecho segundo cuál debe ser la información que debe requerirse a la Policía, en el caso en que solicitase la intervención: «la Policía solicitante la expresión de *la noticia racional* del hecho delictivo a comprobar y *la probabilidad* de su existencia, así como de la *implicación* posible de la persona cuyo teléfono es el objeto de la

En todos los casos, el Juez Instructor, tiene la potestad de pedir un complemento o adición al oficio, si alguno de los aspectos no queda lo suficientemente claro.

(ii) El apartado segundo es el que justifica la existencia de la obligación de explicación y de justificación a las que más arriba se aludió al hablar de la motivación aplicada a los investigadores. Se exige por la LECrim razones justificadas que determinen la existencia de un delito, pero también se exigen dichos razonamientos sobre la conveniencia de la realización de la diligencia solicitada, de su necesidad y de su ajuste a los principios rectores. Esto debe conllevar una actividad explicativa y razonadora aplicada a los hechos concretos que son objeto de investigación. Para cumplir con esta finalidad la LECrim exige explicar qué diligencias se han llevado a cabo hasta el momento[170] de la solicitud, cuál ha sido el resultado obtenido y cómo estas sirven como indicios de la comisión de la acción ilícita investigada.

(iii) El contenido del apartado tercero puede, a priori, resultar redundante con respecto al contenido del apartado primero, porque exige el suministro de los datos del investigado. Sin embargo, no es así. El apartado primero habla de identidad, mientras que el tercero se refiere a datos, y pone este vocablo en relación con la expresión *"medios de*

---

intervención. Los datos que deben ser facilitados por la Policía tienen que tener una *objetividad* suficiente que los diferencia de la mera intuición policial o conjetura. Tienen que ser objetivos en el doble sentido de ser a*ccesibles* a terceros y, singularmente, *al Juez* que debe autorizarla o no, pues de lo contrario se estaría en una situación ajena a todo posible control judicial, y es obvio que el Juez, como director de la encuesta judicial no puede adoptar el pasivo papel del vicario de la actividad policial que se limita a aceptar sin control alguno lo que le diga la policía en el oficio, y obviamente, el control carece de ámbito si sólo se comunican intuiciones, opiniones, corazonadas o juicios de valor.
En segundo lugar, tales datos han de proporcionar una base real suficiente para poder estimar que se ha cometido o se va a cometer el delito que se investiga y de la posible implicación de la persona concernida.
En definitiva, en la terminología del TEDH se deben facilitar por la autoridad policial las " *buenas razones" o "fuertes presunciones* " a que dicho Tribunal se refiere en los casos Lüdi --5 de junio de 1997--, o Klass --6 de septiembre de 1998--. Se trata de términos semejantes a los que se emplean en el art. 579 LECriminal» .

[169] STS 203/2015, de 23 de marzo. Ponente: Don Julián Artemio Sánchez Melgar. Esta sentencia alude a la doctrina que que impide estimar como un indicio de criminalidad la simple alusión a fuentes confidenciales de la policía. «*la mera mención de fuentes confidenciales no es suficiente para justificar tal invasión en los derechos fundamentales y así se ha pronunciado esta Sala en numerosas ocasiones, como es exponente la Sentencia 1497/2005, 13 de diciembre , en la que se recordaba que las noticias o informaciones confidenciales, aunque se consideren fidedignas, no pueden ser fundamento, por sí solas, de una medida cautelar o investigadora que implique el sacrifico de los derechos fundamentales (cfr. STC 8/2000, 17 de enero). Igualmente, no será suficiente por regla general, con la mención policial que se limita a justificar la petición en alusión a «fuentes o noticias confidenciales». Si la confidencialidad está en el origen de la noticia policial de la perpetración delictiva para justificar la medida, habrá de ir acompañada de una previa investigación encaminada a contrastar la verosimilitud de la imputación. Confidencia, investigación añadida y constatación que habrán de estar reseñadas en el oficio policial y que habrán de venir referidas tanto al indicio del delito como de su atribución a la persona a la que va a afectar la medida. En este mismo sentido se han expresado, entre otras muchas, las SSTS 1047/2007, 17 de diciembre y 25/2008, 29 de enero ; 141/2013, 15 de febrero y 121/2010, 12 de febrero*».

[170] En este sentido en la práctica suelen ofrecerse datos acerca de seguimientos realizados, aportando fotografías de los mismos, datos policiales, esquemas policiales referentes a posibles organizaciones adoptadas por los investigados, datos patrimoniales, etc.

comunicación empleados, que permitan la ejecución de la medida". La ley se refiere así a aquellos datos, como el IMEI, el número de teléfono, el correo electrónico, o cualquier otro que se pudiera emplear para realizar la actividad ilícita, y que es el objeto de la diligencia de investigación. Cabe aquí la posibilidad de solicitar del Juez Instructor la expedición de los oficios necesarios para determinarlos, si no fueran conocidos.

(iv) El ordinal cuarto se refiere a qué concreta medida se solicita, y qué extensión debe tener ésta. Con ello se refiere a qué concreta diligencia es la que se interesa de todas las que se contienen en la LECrim, y en cuanto a su extensión la ley se refiere a qué concreto aspecto debe ser el objeto de la limitación del derecho implicado[171]. Además de los aspectos generales, que son comunes a todas las diligencias de investigación, el oficio debe detenerse especialmente en la concurrencia de los requisitos propios y específicos de cada diligencia. En este trabajo tendrá ocasión de ser analizada esta cuestión cuando se estudie la diligencia de acceso y registro remoto de equipos electrónicos. En este apartado puede hacerse alusión al ámbito de producción del delito relacionado con la actividad tecnológica, como modo de justificar la concreta medida que se pide, el concreto tipo penal puesto en relación con dicho aspecto, y las evidencias encontradas que unan ambos argumentos.

(v) El apartado quinto obliga a fijar en el oficio una identificación subjetiva de los encargados de llevar a cabo tales diligencias. Aunque se volverá sobre ello en el estudio de cada diligencia de investigación que se analice, lo que se hace en este apartado es exigir que se determine qué concreto grupo, dentro del cuerpo policial que está investigando los hechos, será el encargado de realizar la medida. Se trata de dar respuesta a la pregunta de quién es el que la llevará a cabo, de manera que el Instructor sepa en todo momento a quien dirigirse, al tiempo que dota de certeza y seguridad jurídica al resultado obtenido, pues de este modo se permite una mejor forma de ser objeto de impugnación.

(vi) El contenido del apartado sexto está referido a la forma de ejecutar la diligencia. En este sentido se han de aportar al Juez Instructor los mecanismos elegidos para llevar a cabo la diligencia[172]. La información suministrada sobre este concreto aspecto permite hacer un

[171] Sirvan de ejemplo la información que se suministra para determinar las concretas conversaciones que se solicitan, en qué días se realizaron, con qué números de teléfono, qué tipos de archivos electrónicos se quieren examinar, con qué tipo de extensión, de que fechas, etc.

[172] Sin ánimo de resultar exhaustivo sirven como ejemplo, concretar en el oficio qué programa se empleará para hacer las escuchas telefónicas, el método de registro del dispositivo de almacenamiento, el programa empleado para registrar un ordenador, la baliza que se empleará para seguir un concreto vehículo, etc.

seguimiento durante la ejecución, y también después de la misma, dirigido a verificar la correcta realización de la diligencia conforme a dicho contenido, de manera que se haya ajustado al mismo.

Considero que dentro del contenido de este apartado se debe admitir cualquier información que permita al Juez Instructor conocer qué información pudiera estar alojada en la nube. La alusión que se hiciera sobre concreto aspecto alerta sobre las posibles respuestas procesales que se pueden dar, tales como solicitar más información a los investigadores, recabar auxilio judicial internacional, instar la información a través del domicilio que la empresa suministradora del servicio pueda tener en España, o cualquier otra. Es importante, a la hora de determinar qué extensión debe abarcar la medida, tener conocimiento sobre la concreta ubicación de los datos, y con ello articular loes medios concretos para su aportación a las actuaciones.

(vii) El apartado séptimo hace alusión a la duración de la medida, con lo que deben suministrarse no sólo los parámetros temporales propiamente dichos, sino también las razones por las que se consideran que los mismos son los más adecuados. El aspecto temporal que se incluye en este apartado es igualmente aplicable al periodo temporal elegido para ir informando del resultado de la diligencia durante su ejecución[173], y también a los casos en que una vez acordada la diligencia, lo que se interesa es una posterior prórroga. Caso de que se interese dicha ampliación deben aportarse las razones y justificaciones para ello así como los nuevos parámetros que justifiquen un mayor o menor lapso en la duración de la ejecución de la diligencia. También se pueden incluir dentro de este apartado una enumeración de las medidas que se llevarán a cabo por parte de los investigadores en el caso de que la diligencia no de el resultado esperado, incluso aunque el plazo temporal concedido no se haya agotado por completo, los periodos propuestos para ir dando cuenta de los resultados obtenidos, así como cualquier otro elemento relacionado con la aplicación de la diligencia en el tiempo.

(viii) Por último, el apartado octavo, guarda relación con las obligaciones que la ley permite imponer a terceros, y que más adelante se analizarán. En todo caso resumidamente, se puede decir en este momento que la ley admite actualmente, obligar a terceros a que conserven la información objeto de búsqueda, o bien permite imponer a personas con conocimientos técnicos adecuados, y relacionados con la información a obtener, que

[173] Por ejemplo, se indicará en el oficio si el Juez será informado sólo mediante un extracto de las conversaciones obtenidas mediante una intervención telefónica, o bien se aportarán completamente transcritas, o si bien se dejarán excluidas las conversaciones o los datos sin trascendencia para la investigación, o cualquier otro aspecto similar a este.

ayuden a los investigadores a extraerla de los equipos en que se encuentran y facilitarla. El contenido de este apartado lo que impone es la obligación de aportar en el oficio de solicitud de la diligencia, los datos de la persona que tendrá la obligación de conservar los datos del sistema intervenido, o cualquier otra obligación similar, de manera que se pueda hacer ésta la advertencia expresa en la resolución judicial, tanto de las obligaciones que le impone la LECrim, así como de sus consecuencias en el caso de que no las verifique correctamente.

En resumen, puede concluirse del tenor literal de la ley, una importante descripción del contenido mínimo que debe tener el oficio policial que interese la medida que tenga potencial para interferir en el contenido de los derechos del art. 18 CE. Si bien no puede hablarse de exhaustividad, en realidad si que se ofrecen las pautas que guían el suministro de información inicial. Esta información que se tiene que suministrar tiene el carácter de mínimo, y no existe inconveniente en que se ofrezca más de lo que se ha expuesto. Además, debe ser una información que se aporte debidamente relacionada y estructurada en relación con los hechos que se investigan. Es decir, debe ser una información que se aporte de manera que el Juez Instructor pueda ponerla en relación con la actividad motivadora que le corresponde realizar cuando dicta el auto que acuerde la diligencia. De ahí que pueda hablarse de cierto correlato entre la actividad de suministro de información en el oficio, con la estrictamente judicial, si bien circunscrita a la que corresponde con el dictado del auto. Aunque las dos actividades no son iguales, ya que una consiste en solicitar y la otra en decidir, puede decirse que en los dos casos el legislador impone, como una seña de identidad de esta reforma, la obligación de abundar en las razones tanto para solicitar la medida, como a posteriori acordarla.

3.1.1. Especial mención a las funciones de la Fiscalía Europea relacionadas con las diligencias de investigación electrónica.

En el seno de este apartado, dedicado a los posibles agentes que han sido habilitados por la ley para pedir la medida de investigación electrónica oportuna, ha surgido un nuevo sujeto habilitado para hacerlo. Este nuevo agente se ha creado dentro de los instrumentos normativos desarrollados en el ámbito de la Unión Europea.

La creación del Espacio de Seguridad y Justicia europeo comporta el desarrollo de estrategias que pretenden homogeneizar las normas y procesos de investigación, de modo que se hagan comunes

para los distintos países que forman parte de ese espacio. La finalidad es que todos ofrezcan a sus ciudadanos el mismo grado de seguridad y de respeto por los derechos individuales, y se mejore la investigación criminal.

En cumplimiento de esa finalidad hay que destacar la aprobación del Reglamento 2017/1939, de 12 de octubre de 2017, por el que se establece una cooperación reforzada para la creación de la Fiscalía Europea[174]. Dentro del contenido de este Reglamento hay aspectos que tienen importante relación en lo que a la investigación tecnológica se refiere.

En primer lugar, se debe tener presente que el contenido de esta norma[175] colisiona con el actual sistema acusatorio español. Puesto que nuestro sistema está basado en la atribución a un órgano jurisdiccional de las funciones de instrucción y de investigación de los actos de relevancia penal, estando diferenciado este órgano de aquél que está encargado del enjuiciamiento.

En cambio, en la mayor parte de países que conforman la Unión Europea, el sistema seguido no es ese, y son más los países en los que las funciones de instrucción de los delitos se atribuyen al Ministerio Fiscal y no a un Juez. En estos países el papel de los jueces es servir de garantes de los derechos de los investigados, velando porque no se vulnere ningún derecho individual.

La regulación procesal española no desconoce este segundo sistema, porque es el que se sigue en determinadas jurisdicciones, como la de menores, pero lo hace de modo residual y circunscrito, como se ve a determinadas jurisdicciones. La elección de un sistema de investigación dirigida por el fiscal ha sido una de las principales ideas rectoras de la reforma, no aprobada, de la Ley de Enjuiciamiento Criminal que se contenía en el Anteproyecto de Código Procesal penal[176]. En ese

---

[174] Esta publicado en el BOE de fecha 31 de octubre de 2017. Enlace web: http://www.boe.es/diario_boe/txt.php?id=DOUE-L-2017-82123.

[175] El Reglamento dedica el artículo 120 a los aspectos relacionados con su entrada en vigor disponiendo que: *«1. El presente Reglamento entrará en vigor a los veinte días de su publicación en el Diario Oficial de la Unión Europea. 2. La Fiscalía Europea ejercerá su competencia respecto de todo delito que le competa y se haya cometido después de la fecha de entrada en vigor del presente Reglamento. La Fiscalía Europea asumirá las funciones de investigación y ejercicio de la acción penal que le otorga el presente Reglamento a partir de una fecha que se determinará mediante una decisión de la Comisión sobre una propuesta del Fiscal General Europeo una vez que se cree la Fiscalía Europea. La decisión de la Comisión se publicará en el Diario Oficial de la Unión Europea. La fecha que deberá fijar la Comisión no será anterior a tres años después de la entrada en vigor del presente Reglamento. Para los Estados miembros que participen en una cooperación reforzada en virtud de una decisión adoptada de conformidad con el artículo 331, apartado 1, párrafos segundo o tercero, del TFUE, el presente Reglamento será aplicable a partir de la fecha indicada en la decisión en cuestión. El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en los Estados miembros de conformidad con los Tratados».* La cuestión de esta entrada en vigor debe ponerse en relación con el conjunto de países que han suscrito este sistema de cooperación reforzada, y que son los que en un primer momento se verán afectados directamente por su contenido. Estos países son Alemania, Bélgica, Bulgaria, Chipre, Croacia, Eslovaquia, Eslovenia, España, Finlandia, Francia, Grecia, Lituania, Luxemburgo, Portugal, República Checa y Rumanía.

[176] En el citado anteproyecto se destacaba en los artículos 38 y 55 la atribución a los Tribunales de garantías los aspectos relacionados con el conocimiento de la fase de investigación, siendo que es el fiscal el encargado de esclarecer los hechos y buscar indicios y daros de éste y de los responsables.

proyecto la instrucción era atribuida al Fiscal, pero se trata de un proyecto que finalmente no se aprobó.

El hecho de que entre los países que conforman el espacio de seguridad común, sean mayoritarios los que atribuyen al Fiscal la instrucción de los delitos, puede haber incidido en la creación de una Fiscalía Europea[177]. Es una figura que queda circunscrita al ámbito geográfico de dieciséis países de la Unión Europea, y que ve limitada sus funciones a determinados ámbitos de investigación.

Entre las características más importantes de esta nueva Fiscalía está el hecho de estar dotada de personalidad jurídica propia, y de contar con su propio estatuto regulador. Los principios que guían su actuación son el de legalidad, proporcionalidad e imparcialidad[178]. En el desarrollo de su actividad debe interactuar conjuntamente con la oficina Eurojust a los efectos de investigar y perseguir los *«delitos que perjudiquen a los intereses financieros de la Unión previstos en la Directiva (UE) 2017/1371 y determinados por el presente Reglamento, así como de ejercer la acción penal y solicitar la apertura de juicio contra sus autores y los cómplices de estos»*[179]. Este puede ser el primer aspecto a destacar, el que su finalidad se limite a la investigación de todo hecho con relevancia penal y trascendencia económica.

El texto del reglamento no limita el número de delitos que pueden ser objeto de investigación. Se permite investigar cualquier tipo penal que tenga relación con intereses financieros susceptibles de ser perjudicados. La expresión "afectación de intereses económicos" es tan amplia que admite muchos tipos de delitos que, en su ejecución, pueden afectar a estas materias: estafas, prevaricación, cohecho, delitos mercantiles, etc. En el preámbulo, anticipándose a lo difuso de la expresión, se ha incluido la posibilidad de que el objeto de la investigación se extienda a los llamados *«delitos indisociablemente vinculados»* a esos intereses económicos.

La Fiscalía europea cuenta, entre sus funciones, la de investigar delitos perpetrados utilizando organizaciones con finalidad delictiva. En este caso sus actividades deben estar expresamente conectadas con los delitos de trascendencia económica. Para el cumplimiento de las funciones encomendadas a esta Fiscalía se atenderán a los principios de independencia, proporcionalidad, equidad e imparcialidad hacia el sospechoso, y respetando el principio de legalidad a la hora de proceder en la ejecución de tales actividades, así como evitando dilaciones indebidas[180].

---

[177] En el Diario Oficial de la Unión Europea de 30/10/2017 se ha publicado el REGLAMENTO (UE) 2017/1939 DEL CONSEJO de 12 de octubre de 2017 por el que se establece una cooperación reforzada para la creación de la Fiscalía Europea.

[178] Ver arts. 5.2 y 5.4 del Reglamento 2017/1939, de 12 de octubre

[179] Ver art. 4 del Reglamento 2017/1939.

[180] Son las palabras extraídas del considerando 65 y 66 del Reglamento, puestas en relación con el contenido del artículo 5 de esa misma norma.

En uso de la independencia que le es atribuida puede iniciar las investigaciones de manera autónoma y por cuenta propia, siempre que, bajo su parecer, existan «*motivos razonables*»[181] para hacerlo. Tales investigaciones se pueden encomendar al Fiscal delegado en cada país integrante, quien puede culminarlas por sí mismo, o bien encomendarlas a que sean las autoridades nacionales del país en el que se encuentra para que las realice. Esta facultad se denomina derecho de avocación o traslación de funciones, que se encuentra expresamente regulado en la norma[182] . El criterio de funcionamiento que se fija es que la Fiscalía europea es la competente para investigar los delitos cuyo examen tiene atribuidos, salvo que decida que el asunto objeto de investigación ha de ponerlo en conocimiento de las autoridades nacionales para que sean ellas las que investiguen estos hechos. La norma somete a un plazo muy breve la exteriorización de esta voluntad de investigar o de no hacerlo, pues exige por un lado que se disponga lo antes posible y no podrá hacerlo pasados cinco días desde que conoció el asunto a investigar.

La doctrina resalta la contraposición de modelos de acusación entre el sistema previsto en este Reglamento de la Unión Europea y las leyes españolas. El modelo de fiscalía española no está aún adaptado para ser el órgano encargado de la instrucción, como se preveía en el Anteproyecto de Código Procesal penal, lo que puede implicar problemas en la aplicación práctica de la figura y en su consolidación futura, pues *«esta nueva regulación supondrá un revulsivo para aquellos modelos en los que como en el nuestro, las facultades de control de la instrucción en el ámbito de la justicia penal continúa en poder de los Jueces de Instrucción, lo que conllevará de forma irremediable a un cambio en el modo de entender la justicia penal»*[183].

Entre las facultades del nuevo Fiscal Europeo hay algunos aspectos que se refieren específicamente a las diligencias de investigación tecnológica. Y es que, para la ejecución de las funciones de investigación que le son atribuidas por parte de sus normas específicas, se admite que puedan llevarse a cabo toda clase de acciones de indagación e investigación, que deben respetar el principio de proporcionalidad[184], es decir, tal y como ya se vio en otro apartado, siempre que existan medidas de investigación menos intrusivas en los derechos del investigado, que permitan obtener el mismo resultado, serán estas últimas las que se realicen[185]. También se ha de atender a la gravedad del asunto y a los demás derechos implicados.

---

[181] Se explicita textualmente esta facultad en los arts. 26 y 28 del texto del Reglamento.
[182] En concreto se detalla en el art. 26 del texto legal.
[183] Cfr. DORESTE ARMAS, Delia Carolina. «El espacio judicial europeo y la fiscalía europea como órgano de investigación y persecución penal; versus modelo procesal español». *Diario La Ley*, Nº 8981, 17 de Mayo de 2017. Pág. 8.
[184] Considerando 70 del reglamento. Lo que deba ser entendido por proporcionalidad puede completarse con el contenido jurisprudencial y legal sobre el particular.
[185] Ver el art. 30.5 del Reglamento.

Las diligencias que están enumeradas en el reglamento no constituyen un listado cerrado, ni un *numerus clausus*. Al contrario. Las facultades de estos fiscales son muy amplias y emanan tanto de su Reglamento regulador como las que permite realizar el derecho nacional propio del Estado en el que se ha llevado a cabo la acción penal objeto de persecución. La ejecución y práctica concreta de diligencias deberá ser permitida y contemplada por el Reglamento, pero además la práctica concreta de dicha diligencia ha de hacerse siguiendo el contenido de las normas procesales de cada uno de los países integrantes del espacio común que han ratificado el contenido del Reglamento creador de esta Fiscalía[186]. El Fiscal europeo dispone además, para investigar los hechos penales de su competencia, de todas las diligencias de investigación que no estando contempladas en su propia regulación, sí que lo están en las normas procesales nacionales del propio país donde se está investigando.

Las diligencias de investigación que se pueden llevar a cabo por parte de la Fiscalía Europea se contemplan en el texto legal de un modo muy exhaustivo[187], pero no hay que olvidar que ha de contarse con las normas procesales nacionales, que deben admitir su ejecución.

---

[186] Art. 30.2, 3 y 4 del Reglamento.

[187] El artículo 30 del Reglamento 2017/1939 enumera tales diligencias. Resulta de interés transcribir su contenido por el elevado número de diligencias que ejemplifican el acceso, tanto físico como remoto, a diferentes clases de dispositivos de información. Dispone dicho artículo bajo la rúbrica *«Medidas de investigación y otras medidas 1. Al menos en los casos en que el delito objeto de la investigación sea punible con una pena máxima de al menos cuatro años de prisión, los Estados miembros garantizarán que los Fiscales Europeos Delegados estén facultados para ordenar o solicitar las siguientes medidas de investigación: a) inspeccionar cualquier local, territorio, medio de transporte, domicilio privado, ropa y pertenencias personales o sistemas informáticos, y adoptar todas las medidas cautelares necesarias para preservar su integridad o evitar la pérdida o contaminación de pruebas; b) conseguir la presentación de cualquier objeto o documento pertinente, ya sea en su formato original o en otro formato determinado; c) conseguir la presentación de datos informáticos almacenados, ya sean encriptados o descifrados, en su formato original o en otro formato determinado, incluidos los datos relativos a cuentas bancarias y de tráfico, con la excepción de los datos específicamente conservados de conformidad con el Derecho nacional en aplicación del artículo 15, apartado 1, segunda frase, de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo; d) inmovilizar los instrumentos o los productos del delito, incluidos los activos, si se prevé que el órgano jurisdiccional los decomisará y si existen motivos para pensar que el propietario, poseedor o gestor de dichos instrumentos o productos intentará frustrar la sentencia que ordene su decomiso; e) interceptar las comunicaciones electrónicas enviadas y recibidas por el sospechoso o el acusado, a través de todo medio de telecomunicaciones electrónicas que utilice el sospechoso o el acusado; f) seguir y localizar un objeto por medios técnicos, incluidas las entregas controladas de mercancías.*

2. Sin perjuicio de lo dispuesto en el artículo 29, las medidas de investigación establecidas en el apartado 1 del presente artículo podrán estar sujetas a condiciones de conformidad con el Derecho nacional aplicable si este contiene restricciones específicas que se aplican respecto de determinadas categorías de personas o profesionales que están sometidas a una obligación de confidencialidad jurídicamente vinculante.

3.Las medidas de investigación establecidas en el apartado 1, letras c), e) y f), del presente artículo podrán estar sujetas a otras condiciones, incluidas limitaciones, previstas por el Derecho nacional aplicable. En particular, los Estados miembros podrán restringir la aplicación del apartado 1, letras e) y f), del presente artículo, a delitos graves específicos. Un Estado miembro que tenga la intención de hacer uso de esa limitación notificará a la Fiscalía Europea la correspondiente lista de delitos graves específicos de acuerdo con el artículo 117.

4. Los Fiscales Europeos Delegados estarán facultados para solicitar u ordenar cualesquiera otras medidas a las que puedan recurrir los fiscales en su respectivo Estado miembro en casos similares en virtud del Derecho nacional, además de las medidas indicadas en el apartado 1.

5.Los Fiscales Europeos Delegados solo podrán ordenar las medidas a las que se refieren los apartados 1 y 4 cuando existan motivos razonables para creer que la medida específica de que se trate podría facilitar información o aportar pruebas útiles para la investigación, y cuando no quepa recurrir a medidas menos intrusivas que puedan lograr el

La enumeración de diligencias que contiene el Reglamento 2017/1939 reúne algunos ejemplos de medidas relacionadas con el registro y acceso de datos albergados en dispositivos tanto físicos como virtuales. En este sentido, la Fiscalía europea está facultada, entre otras diligencias, para instar la inspección de un sistema informático, con la posibilidad de solicitar su bloqueo para evitar la pérdida de indicios. Puede solicitar que le sean exhibidos los datos informáticos (en tanto que posibilita a exhibición de documentos en cualquier formato) y más específicamente aquéllos que estando almacenados pudieran estar encriptados.

El art. 30.1.c) del Reglamento resulta especialmente importante en el objeto de estudio de esta tesis. Dicho precepto habilita al Fiscal europeo para poder acceder a datos que se encuentren almacenados, estén o no encriptados, incluyendo datos económicos y cuentas bancarias. Se excluyen los datos que puedan estar protegidos por la legislación nacional. El supuesto de hecho contemplado por el Reglamento admitiría la posibilidad de que se pudieran obtener datos almacenados en la nube, si bien habría que estar a la posible naturaleza de dichos datos, y su ubicación, para ver si es necesario acordar dicha diligencia acudiendo a la legislación nacional, que en el caso de España sería la que se regula en la LECrim y que es la especialmente referida a los dispositivos de almacenamiento de datos o al registro remoto de equipos informáticos, en la medida en que dichas disposiciones son las que la ley nacional contempla para limitar el derecho a la intimidad o el derecho al entorno virtual, en el caso en que fuera más de uno, los derechos afectados. En esos casos, el Fiscal Europeo, en el caso de investigar un delito cometido en España, y en el que se quiera acudir a esta clase de datos, se puede valer con carácter general, de su habilitación reglamentaria, y acudir al supuesto concreto previsto en la legislación procesal española.

En lo que afecta a las comunicaciones, puede instar que se proceda a la intervención de las del sospechoso o también realizar seguimientos al investigado, mediante sistemas de balizamiento y localización.

El Fiscal europeo está habilitado también para inspeccionar objetos, datos personales del investigado, y sistemas informáticos. La facultad del Fiscal para realizar una diligencia consistente en el acceso a dispositivos de almacenamiento masivo de información, que le sea presentado su contenido, así como el de los datos contenidos dentro de ellos está comprendida dentro de este apartado. No hay alusión expresa a la facultad de intervenir remotamente equipos, pero sí la facultad de intervenir comunicaciones realizadas a través de cualquier medio (incluyendo por consiguiente el que se realiza empleando un ordenador). En cualquier caso, aunque no le está

---

mismo objetivo. La legislación nacional aplicable regirá los procedimientos y las modalidades para adoptar las medidas».

reconocida esa facultad de manera expresa por parte del reglamento, pero conforme al mismo puede hacer uso de las facultades reconocidas por dicho reglamento, y para el caso de España, y siendo esta una diligencia admitida por la ley nacional, puede apoyarse en la legislación procesal penal interna e instar el registro remoto de un equipo, si la investigación se refiere a territorio español.

En la norma también se destaca una gran sensibilidad hacia la protección de los datos que se emplean durante la investigación. Las actividades de averiguación propias de la Fiscalía conllevan, necesariamente, el empleo de los datos de las personas (físicas y jurídicas) investigadas. En la regulación de esta institución la preocupación por la protección de los datos tiene un claro fundamento, porque la Fiscalía es creada para investigar delitos que afectan a intereses financieros en los que se manejan muchos datos. Específicamente, los delitos financieros y económicos exigen el examen de mucha información, así como de multitud de datos diversos como la contabilidad, declaraciones fiscales, declaraciones a la seguridad social, relación de empleados, de clientes, de proveedores, datos bancarios, entre otros, por eso es comprensible que la norma dedique al tratamiento de datos una extensa regulación[188].

La mención al tratamiento de los datos incluye diferentes definiciones de conceptos muy consolidados en el ámbito de la protección de datos entre otros, datos personales, tratamiento, limitación de tratamiento, y muchos otros que actúan a modo de glosario de definiciones. El Reglamento también incluye algunas categorías conceptuales relacionadas con investigaciones de naturaleza tecnológica como el concepto de elaboración de perfiles o seudonimización[189].

La Fiscalía europea, para llevar a cabo sus funciones y usar los datos con los que cuente, debe actuar de manera coordinada con el Supervisor Europeo de Protección de datos. Está obligada a poner en conocimiento del interesado la existencia de los datos que tengan sobre el mismo, lo que podrá verse limitado debido a los intereses de la investigación que se lleve a cabo, así como las necesidades de seguridad nacional, salud nacional, etc. Es decir, se ve obligada a efectuar una comunicación de los datos que posea de los investigados y afectados.

Esta obligación también se contempla en la LECrim española aunque ceñida exclusivamente al ámbito de las grabaciones de comunicaciones adoptadas en el seno de un proceso penal; en todo

[188] El Capítulo VII del reglamento contiene las disposiciones referentes al tratamiento de la información de la que hace uso de la Fiscalía europea. Dicho tratamiento es un modo de asegurar una protección de datos adecuada. Se contiene en los arts. 43 a 46. Por otro lado el Capítulo VIII contiene una regulación más específica y detallada sobre la protección de datos personales en los arts. 47 a 89. Se dedican cuarenta y dos artículos a regular cuestiones como las transferencias de datos, la comunicación a terceros de la disposnibilidad de los mismos, así como numerosas cuestiones más relacionadas con dichos datos, que son directamente exigibles a los Fiscales Europeos en el desarrollo de su labor.
[189] Ver el art. 2 del Reglamento 2017/1939.

caso se trata del único caso que puede asimilarse a la obligación de comunicación de datos que hay en la legislación procesal penal española, lo que supone en todo caso un aspecto muy importante[190].

El Reglamento dedica además otros preceptos a la colaboración con el órgano encargado de la supervisión de estos datos a nivel europeo, e incluso abre a la posibilidad de que el tratamiento de datos regulado en el Reglamento de protección de datos 2016/679, sea modificado a los efectos de contemplar esta capacidad de investigación de la Fiscalía.

En todo caso, lo destacable es que se contiene una regulación muy sensible hacia el respeto de los datos personales de terceros, y más en el seno de un órgano de esta naturaleza, y este aspecto probablemente marque una tendencia en los posibles desarrollos que una futura legislación procesal nacional pueda aportar sobre este particular.

Lo anterior sirve para colegir que el Fiscal Europeo podrá ser también uno de los solicitantes de la ejecución de las medidas de investigación tecnológica previstas tanto en nuestras leyes procesales, como en el reglamento que regula dicha Fiscalía. En este segundo caso debe estar prevista su ejecución por las normas procesales españolas.

3.2. Audiencia del Ministerio Fiscal.

La petición de práctica de cualquier diligencia de investigación electrónica, por parte de las Fuerzas y Cuerpos de Seguridad del Estado, requiere que, conforme al contenido del art. 588 bis c LECrim, se de audiencia al Ministerio Fiscal. La finalidad de esta audiencia es que el fiscal se pronuncie sobre la procedencia o no de acordar la medida solicitada. Debe entenderse que esta petición también será posible en el caso de que la medida de investigación parta de la iniciativa de oficio del Juez Instructor[191].

La actual audiencia preceptiva termina con la interpretación, que hasta ahora se sostenía, conforme a la cual no resultaba necesario darle traslado, en la medida en que el Ministerio fiscal intervenía necesariamente en el procedimiento penal y con ello iba a estar al tanto de la resolución que se dictara caso a caso.

En el supuesto en que el solicitante de la medida sea el propio Ministerio Público, no debe darse cauce a este trámite, dado que en ese caso ya conocería los hechos, su alcance, y la necesidad de

[190] El Capítulo VIII, que comprende los arts. 47 a 89, son los que determinan el tratamiento de la información que se pone a disposición de la Fiscalía Europea. En el caso de la legislación española que permite comunicar a terceros la existencia de grabaciones de comunicaciones en las que ha participado, se contempla en el art . 588 ter, i) 3 de la LECrim.
[191] Circular de la Fiscalía General del Estado 1/2019, de 6 de marzo. Pág. 13.

realizar diligencias de investigación. Esta audiencia, como trámite ineludible, se ha creado para dar posibilidad de pronunciarse sobre ella a quien no conoce, hasta ese momento, la petición de intervención, y quien debe velar por el respeto de los derechos fundamentales de los investigados. De ahí que no parezca necesario dar trámite en los casos en que el propio Ministerio Público (también en el caso del Fiscal Europeo) sea quien interesa la intervención, y donde lógicamente se habrá pronunciado, motivado y fundado todo lo procedente sobre la adopción de la medida[192].

Nada dice la ley sobre cómo han de entenderse los efectos derivados de la falta de esta petición de informe previo. En este sentido, no parece que la consecuencia deba ser la nulidad, porque el Ministerio Fiscal, una vez notificado de la resolución que la acuerde, puede recurrir su contenido, en todo caso, con relación a la consecuencia derivada de la falta de notificación y audiencia el Fiscal, la propia Circular de la Fiscalía General del Estado 1/2019, considera que debería ser considerado como una mera irregularidad procesal.

3.3. Forma de la resolución, contenido y plazo.

[192] STS 272/2017, de 18 de abril. Ponente: Don Juan Saavedra Ruíz. La sentencia contiene en su fundamento 2.5 un pronunciamiento específico sobre la intervención del Ministerio Fiscal en las actuaciones consistentes en decisiones sobre intervenciones de telecomunicaciones tanto antes como después de la reforma operada por la Ley Orgánica 13/2015. Dispone lo siguiente: «*2.5. En relación con la falta de notificación del auto al Ministerio Fiscal la queja tampoco puede ser aceptada. Con anterioridad a la reforma de la Ley de Enjuiciamiento Criminal (L.O. 13/2015) no era preceptivo el informe del Fiscal para la adopción de una medida de injerencia en los derechos fundamentales proclamados por el artículo 18 CE , de forma que el conocimiento de la resolución dio lugar a cierta controversia jurisprudencial, desde una interpretación rigurosamente formalista que exigía su notificación al Ministerio Fiscal a una segunda línea, plenamente consolidada, que flexibiliza lo anterior por cuanto de lo que se trata es de evitar decisiones cuasiclandestinas en el curso de la instrucción, sobre todo cuando las mismas se adoptaban en el seno de unas indefinidas diligencias indeterminadas. Por ello la exigencia de la notificación formal fue relativizada por la jurisprudencia constitucional (ver STC 25/2011) y del Tribunal Supremo desde hace ya algunos años (SSTS 138/2006 , 1013/2007 , 578/2009 , 309/2010 o 385 y 694/2011), donde decíamos que el Fiscal no necesita de un acto formal de invitación al proceso puesto que su presencia es institucional y conforme al artículo 306 LECrim . los Jueces de Instrucción formaran los sumarios bajo la inspección directa del Fiscal del Tribunal competente, de forma que ex artículo 308 LECrim . inmediatamente que aquéllos tuvieren noticia de la perpetración de un delito lo pondrán en conocimiento del Ministerio Fiscal, con cita del artículo 773 LECrim ., concluyendo que su presencia en la fase de investigación y, por tanto, el eficaz ejercicio de las funciones que le incumben, no puede condicionarse al hecho de que exista constancia en la causa de un acto formal de comunicación. El artículo 777 LECrim . impone al Instructor el deber institucional de dar cuenta al Fiscal de la incoación de las diligencias previas y de los hechos que la determinen y el artículo 772 de la misma exige de la policía, en el momento de extender el atestado, remitir copia al Ministerio Fiscal.*
Después de la reforma de la Ley de Enjuiciamiento Criminal (L.O. 13/2015) el legislador ha resuelto cualquier discusión en esta materia cuando en el artículo 588 bis c), bajo la mención de resolución judicial, establece en su apartado I que el Juez de Instrucción autorizará o denegará la medida solicitada (se refiere a las comprendidas en el Capítulo IV) mediante auto motivado, oído el Ministerio Fiscal, excepto naturalmente en aquellos casos en que sea él mismo quien haya instado la diligencia de investigación limitativa de los derechos a que se refiere el Capítulo mencionado».

El auto del Juez instructor sobre la adopción de una diligencia de investigación electrónica ha de ser una resolución razonada, ponderada y motivada suficientemente. Esta exigencia es una garantía para el investigado de modo que pueda conocer el cauce lógico seguido por el órgano jurisdiccional a los efectos de poder controlar jurídicamente su contenido[193].

El legislador se ha asegurado de que la motivación concurra en todo caso. Para ello ha fijado numerosas exigencias que la aseguren, estableciendo el contenido mínimo que ha de reunir un auto que limite cualquiera de los derechos del art. 18 CE. En esa línea es como ha de entenderse el apartado 3 del art. 588 bis c LECrim cuando exige al auto del Juez Instructor, una generosa e importante cantidad de información, con carácter de mínimos.

El auto describirá el hecho que es objeto de investigación, aludirá a su calificación jurídica al menos de forma primaria (conforme a lo que permita el embrionario estado de la investigación criminal), así como la expresión de los indicios racionales tenidos en cuenta para fundamentar la medida. La resolución contendrá la identidad de los investigados y de cualquier otro afectado por la medida, si es que éste fuera conocido. El contenido también habrá de abarcar la extensión de la medida de injerencia, especificando cuál será su alcance y una especial motivación relativa a los principios rectores que se analizaron más arriba y que se contenían en el art. 588 bis a LECrim.

La resolución ha de hacer mención a qué unidad policial es la que se hará cargo de llevar a cabo la intervención[194], la duración que tendrá esta injerencia, y el modo y la periodicidad con la que el órgano que ejecuta la intervención informará al órgano judicial, así como la finalidad que se persigue con la adopción de la medida de limitación de derechos[195].

---

[193] Es reiterada la doctrina tanto del Tribunal Supremo y del Tribunal Constitucional que establece que la obligación de motivación de las resoluciones judiciales entronca con el derecho a la tutela judicial efectiva. En este sentido, sobre este aspecto, cabe citar la reciente STS 200/2017 de 27 de marzo. Ponente: Don Juan Ramón Berdugo Gómez de la Torre, que señala que: «*Como se ha dicho en las SSTS. 29/2010 de uno de febrero y 544/2016 de 21 junio recogiendo la doctrina expuesta en SSTC. 314/2005 de 12 diciembre , 94/2007 de 7 mayo , 160/2009 de 29 junio , el requisito de la motivación de las resoluciones judiciales halla su fundamento en la necesidad de conocer el proceso lógico- jurídico que conduce al fallo y de controlar la aplicación del Derecho realizada por los órganos judiciales a través de los oportunos recursos, a la vez que permite contrastar la razonabilidad de las resoluciones judiciales. Actúa, en definitiva, para permitir el más completo ejercicio del derecho de defensa por parte de los justiciables, quienes pueden conocer así los criterios jurídicos en los que se fundamenta la decisión judicial, y actúa también como elemento preventivo de la arbitrariedad en el ejercicio de la jurisdicción».*

[194] La Circular de la Fiscalía General del Estado 1/2019, de 6 de marzo alude a que este requisito no ha sido nunca exigido por la jurisprudencia.

[195] El contenido de la información que el auto judicial debe ofrecer cuenta con un de mínimo de ésta que debe contener. Esta exigencia de mínimos se extrae de la expresión literal del precepto cuando exige que la resolución contenga "al menos" los extremos que a continuación pasa a enumerar y que son: «*a) El hecho punible objeto de investigación y su calificación jurídica, con expresión de los indicios racionales en los que funde la medida; b) La identidad de los investigados y de cualquier otro afectado por la medida, de ser conocido; c) La extensión de la medida de injerencia, especificando su alcance así como la motivación relativa al cumplimiento de los principios rectores establecidos en el artículo 588 bis a; d) La unidad investigadora de Policía Judicial que se hará cargo de la intervención; e) La duración de la medida; f) La forma y la periodicidad con la que el solicitante informará al juez sobre los resultados de la medida; g) La finalidad perseguida con la medida; h) El sujeto obligado que llevará a cabo la medida, en caso de*

El contenido del art. 588 bis c, apartado h) LECrim, exige que se aperciba al obligado a colaborar en el desarrollo de algún aspecto relacionado con la ejecución de la medida del posible delito de desobediencia en que se podría incurrir de no cumplir con la orden judicial, todo ello en caso de que se conozca. Esta medida puede ser extensible a los colaboradores en la practica de algunas de las diligencias que serían objeto de análisis más adelante. En este caso se habla de terceros que pueden tener en su poder, bien la información, o bien disponen de los conocimientos o los medios tecnológicos para poder extraerla del lugar en la que se ubica. Estas personas, que pueden ser técnicos de entidades o empresas, están obligadas a prestar colaboración a los agentes encargados de la investigación, y por lo tanto deben ser advertidas de las consecuencias de su incumplimiento[196].

Este grado de exhaustividad y detalle que se exige al auto judicial no es una exigencia nueva ni desconocida en nuestro Derecho, pues la necesidad de que el auto contenga información, motivación y razonamiento suficiente, venía siendo requerido, de forma constante, por la jurisprudencia en relación con los medios de investigación limitativos de los derechos de las personas [197]. En todo caso, la información exigida por la ley, lo es con carácter de mínimo, por lo que no hay inconveniente en que el Juez Instructor incremente la información que contiene su resolución. La doctrina de la Sala Segunda no se agota al considerar que es necesario hacer constar suficiente información a los efectos de justificar la adopción de las medidas que se pudieran en cada caso acordar [198].

---

conocerse, con expresa mención del deber de colaboración y de guardar secreto, cuando proceda, bajo apercibimiento de incurrir en un delito de desobediencia».

[196] Sirven como ejemplo de estas obligaciones impuestas a terceros el contenido del art. 588 ter e LECrim en el ámbito de las intervenciones de comunicaciones, y más concretamente en el ámbito de la diligencia de almacenamiento masivo de información se puede citar el art. 588 sexies c, apartado 5, o el art. 588 septies b con respecto a la diligencia de registro remoto de equipos electrónicos.

[197] STS 292/2015, de 14 de mayo. Ponente: Don Joaquín Jiménez García. Considero necesario aludir a que la motivación de la resolución a veces puede llevarse a cabo por referencia al oficio policial que interesa la medida de intervención. Es decir, el Juez instructor motiva su auto incluyendo el contenido del oficio, al cual expresamente se remite. El Tribunal Supremo, como regla general no ve con buenos ojos este modo de motivar las resoluciones judiciales, pues exige del Juez un esfuerzo valorativo y argumentativo personal. Sin embargo se ha venido admitiendo la posibilidad del auto dictado mediante remisión al oficio. Así la sentencia invocada dice: «*Esta sala, en coincidencia con diversa jurisprudencia de amparo, ha declarado en multitud de ocasiones (por todas STS 320/2004, de 17 de marzo y las que en ella se citan) que "los autos que autorizan intervenciones telefónicas pueden ser integrados con el contenido de los respectivos oficios policiales en que éstas se solicitan, de forma que es suficiente la motivación por referencia a los mismos", cuando el auto así integrado contiene los elementos necesarios para hacer posible el ulterior control de necesidad y proporcionalidad de la intervención. Si bien es cierto que, como también se ha dicho, "lo deseable es que la expresión de los indicios objetivos que justifiquen la intervención quede exteriorizada directamente en la resolución»*.

[198] Así, por ejemplo, debe determinarse, con precisión, el número o números de teléfono que deben ser intervenidos, el tiempo de duración de la intervención, quién ha de llevarla a cabo y los periodos en los que deba darse cuenta al Juez de sus resultados a los efectos de que éste controle su ejecución (por todas SSTC 49/1996, de 26 de marzo ; 49/1999, de 5 de abril ; 167/2002, de 18 de septiembre ; 184/2003, de 23 de octubre ; 259/2005, de 24 de octubre ; 136/2006, de 8 de mayo). Esta sentencia se hace eco de numerosa jurisprudencia anterior disponiendo que : *«Sobre esa base, el Tribunal Constitucional ha considerado insuficiente la mera afirmación de la existencia de una investigación previa, sin*

La exigencia por parte de la ley de tanta información que debe contener el auto nos conduce a preguntarnos sobre la consecuencia que se anuda a la inexistencia o a la insuficiencia de la información mínima requerida. Lo reciente de la nueva regulación impide encontrar eco en esta pregunta y menos aún una respuesta en la jurisprudencia del más alto Tribunal, sin embargo, alguna reciente resolución permite considerar la posibilidad de que si el contenido de las decisiones judiciales han sido objeto de precisa y expresa regulación, exigiéndoles a estos autos, una determinada y mínima información que deben contener, puede colegirse que de no observarse tal contenido mínimo, la resolución que la evite pueda llegar a ser nula [199].

El art. 588 bis c LECrim establece que la resolución del Juez instructor sobre la diligencia de investigación, ha de dictarse en un plazo de veinticuatro horas desde la presentación de la solicitud. El plazo se suspenderá cuando el juez instructor requiera alguna aclaración o complemento al oficio presentado. La fijación de un plazo para dictar el auto que admita o rechace la práctica de la diligencia, es un elemento nuevo en nuestra legislación, ya que antes de la reforma este acto no estaba sometido a plazo.

Este nuevo aspecto presenta la ventaja de que la resolución judicial se obtiene en un plazo muy breve, que viene predeterminado por la legislación procesal. No obstante, debe tenerse presente que hay ocasiones en las que el plazo resulta escaso, porque no es igual determinar la información necesaria para acordar un registro telefónico, que la que puede ser necesaria para intervenir remotamente un equipo. En todo caso, el recurso a la exigencia de que sea aportada mayor información, cuando la proporcionada no sea suficiente, actúa de modo acertado para que finalmente el contenido del auto sea el mejor posible, y el más respetuoso con los derechos fundamentales.

---

especificar en qué consiste, ni cuál ha sido su resultado por muy provisional que éste pueda ser, afirmando también que la concreción del delito que se investiga, las personas a investigar, los teléfonos a intervenir y el plazo de intervención no pueden suplir la carencia fundamental de la expresión de los elementos objetivos indiciarios que pudieran servir de soporte a la investigación, ni la falta de esos indispensables datos pueda ser justificada a posteriori por el éxito de la investigación misma (SSTC 299/2000, de 11 de diciembre ; 138/2001, de 18 de junio ; 167/2002, de 18 de septiembre ; 165/2005, de 20 de junio 259/2005, de 24 de octubre ; 253/2006, de 11 de septiembre). También ha destacado que "la idea de dato objetivo indiciario tiene que ver con la fuente de conocimiento del presunto delito, cuya existencia puede ser conocida a través de ella. De ahí que el hecho en que el presunto delito puede consistir no pueda servir como fuente de conocimiento de su existencia. La fuente del conocimiento y el hecho conocido no pueden ser la misma cosa" (STC 299/2000, de 11 de diciembre ; 138/2001, de 18 de junio). Asimismo, debe determinarse con precisión el número o números de teléfono que deben ser intervenidos, el tiempo de duración de la intervención, quién ha de llevarla a cabo y los períodos en los que deba darse cuenta al Juez de sus resultados a los efectos de que éste controle su ejecución (por todas SSTC 49/1996, de 26 de marzo; 49/1999, de 5 de abril; 167/2002, de 18 de septiembre; 184/2003, de 23 de octubre; 259/2005, de 24 de octubre; 136/2006, de 8 de mayo)».

[199] Sentencia de la AP Cáceres , Sección 2º, 12/2017, de 25 de enero. Ponente: Don Jesús María Gómez Flores

3.3.1. El aspecto temporal como presupuesto exigible en el auto.

Por razones de sistemática, y en la medida en que el art. 588 bis c, apartado e) LECrim, recoge que uno de los extremos sobre los que debe pronunciarse el Juez instructor es el relativo a la duración de la medida de investigación que se acuerde, considero que el contenido de los arts. 588 bis, e) y f) LECrim han de ser estudiados aquí. Ambos preceptos contemplan distintas visiones del elemento temporal aplicado a las diligencias de investigación, dado que se dedican a regular la duración de las medidas y la solicitud de prórroga respectivamente.

El elemento temporal de la ejecución de la diligencia, esto es, la duración esperada para llevar a cabo la medida es un aspecto formal que los solicitantes deben tener en cuenta en el oficio, y sobre el que el Juez debe hacer mención y determinación expresa en el auto (art. 588 bis e LECrim). La ausencia de cualquier límite a la duración de la diligencia en cuestión haría que su ejecución se eternizara, lo que contravendría la excepcionalidad de cualquier medida que limite derechos fundamentales. Esto es lo que trata de evitar el legislador ordenando que se acote necesariamente su duración por parte del Juez.

La determinación del elemento temporal de la práctica de una diligencia debe seguir un criterio restrictivo. Por eso no tiene porqué agotarse el plazo marcado en la ley, ni siquiera el otorgado por el Juez, y se puede conceder uno menor, o incluso una vez alcanzada la finalidad de la medida, los investigadores pueden solicitar la revocación de la misma, o cabe inclusive dejar previsto en la resolución que la medida quede inmediatamente sin efecto cuando se obtenga la información que se buscaba. Resulta claro, por tanto, que el plazo legal actúa siempre como plazo de duración máxima.

El art. 588 bis e LECrim, insiste en la idea de que la duración de la medida debe ser un aspecto que debe tratarse con carácter restrictivo, de modo que ésta dure el tiempo *«imprescindible para el esclarecimiento de los hechos».* En todo caso, el plazo temporal, que cada tipología de diligencia de intervención o registro establezca, debe actuar como un límite infranqueable, ya que algunas tipologías de diligencias tienen un plazo de duración más limitado que el general. Esta limitación temporal más acusada puede obedecer a que como la intensidad en la limitación de los derechos afectados es mayor de lo habitual, como contrapartida, se limita, más aún, su duración en el tiempo.

El art. 588 bis, apartado c, 1, también contiene una disposición que afecta al elemento temporal. En concreto, introduce un plazo que obliga al Juez a dictar la resolución sobre la diligencia solicitada, en un plazo de veinticuatro horas. Antes de la reforma, el Juez no se veía vinculado a dictar la resolución que acordase diligencia en ningún plazo. En todo caso, el plazo quedaría en suspenso,

según la doctrina, si el Juez necesita que se amplíe la información que contiene el oficio, antes de pronunciarse. Se dice así que *«el no respeto de este plazo de decisión solamente podría tener incidencia real sobre la validez de la resolución habilitante en tanto en cuanto pudiera afectar a la propia idoneidad de la medida (cuando se dicta la resolución, el acontecimiento concreto por el que se solicita ya habría tenido lugar) o cuando esa dilación, obviamente excesiva y desproporcionada, pudiera poner en cuestión los mismos cimientos en que se fundamentara el presupuesto habilitante»*[200]. Sobre las consecuencias derivadas de la ausencia de observancia del plazo, la Fiscalía General del Estado estima que se trata de una irregularidad procesal, sin mayor trascendencia[201].

Por otra parte, el hecho de que cada investigación sea autónoma hace que mientras que en una pueden obtenerse los resultados esperados a la primera, en otras investigaciones puede que esto no suceda así, pero se sigan dando las circunstancias que aconsejan su mantenimiento. La norma contempla por eso la prórroga de la medida de investigación acordada. El acto de prórroga es también otro aspecto relacionado con el factor tiempo en la práctica de las diligencias de investigación.

La ampliación temporal en la limitación de un derecho fundamental requiere y exige un nuevo ejercicio de motivación del juez instructor. Esta motivación deberá basarse en las circunstancias originarias que se tuvieron en cuenta para acceder a la práctica de la medida y consiste en comprobar si siguen concurriendo. La literalidad de la norma es clara y exige que las circunstancias que se dieron en el auto que acordó la medida, y que sirvieron para acceder a la intervención, sigan dándose cuando se interese la prórroga de ésta[202].

---

[200] Cfr. RODRÍGUEZ LAINZ, José Luis. «Sobre la dimensión temporal de las medidas de investigación tecnológica». Op. Cit. Pág. 10. Además el autor también llama la atención sobre un hecho que parece intrascendente pero que no lo es. Nos dice que mientras para la autorización inicial solo se conceden veinticuatro horas para las prórrogas se concede tanto más, el doble, esto es, cuarenta y ocho horas para el dictar la resolución que concede la prórroga. Además se plantea cuál sería la consecuencia derivada del incumplimiento de este plazo y si ello comportaría la nulidad de la medida, siendo este autor proclive a considerar que no es adecuada una interpretación rigurosa que defienda la aplicación general de la nulidad de la prórroga de la autorización extemporánea, sino que hay que tratar caso a caso atendida la proporcionalidad y las razones que han llevado a ese retraso. De hecho el que la ley permita solicitar más información permite acoger la consideración de que no respetar este plazo tan breve no debe comportar la nulidad per se.

[201] Circular de la Fiscalía General del Estado 1/2016, Pág 19.

[202] Cfr. RODRÍGUEZ LAINZ, José Luis. «Sobre la dimensión temporal de las medidas de investigación tecnológica». Op. Cit. Págs. 4 a 7. Se dice expresamente que *«el peso esencial de ese contenido motivador sigue residenciándose en esa continuidad, subsistencia, en las circunstancias que motivaran su decisión inicial».* Además realiza una interesante labor prospectiva sobre la diferenciación de los aspectos temporales relacionados con el momento inicial de la adopción de la medida, y los diferencia de los aspectos también temporales relacionados con la solicitud de prórroga. Mientras en el primer caso zanja la cuestión acudiendo a la regulación de la LECrim conforme a la cual el inicio del cómputo de la medida es desde el auto que la acuerda, en el segundo caso, es decir, con respecto a las prorrogas alude a las razones que ya fueron tenidas en cuenta para acordar la medida limitadora en su momento inicial.

Para acordar cualquier ampliación, los investigadores (la policía judicial normalmente) han de presentar un nuevo oficio solicitando esta prórroga. El nuevo oficio explicará las razones de la solicitud. Esto, en la práctica, implica informar al Juez Instructor de los resultados obtenidos hasta ese momento, así como de los motivos por los que estiman que debe seguir siendo mantenida la medida. En cualquier caso, los investigadores pueden ponerle fin a la prórroga de la medida adoptada en cualquier momento, si estiman que con ella no se va a obtener el resultado pretendido[203]. Esto puede obedecer a que hayan conseguido el objetivo o entiendan que no se va a obtener. Para el cese de la medida no se necesita motivación pormenorizada al Juez, sino que basta con formular la petición, dado que lo que sí requiere adecuada motivación es la petición de limitación de un derecho para la práctica de una diligencia de investigación, no en cambio la petición de terminación de la medida que supone la restauración de la integridad del derecho que había sido previamente afectado por la investigación.

El desarrollo de la ejecución de la medida durante el plazo concedido inicialmente, no está exento de control, porque el art. 588 bis g) LECrim faculta al Juez Instructor para solicitar información sobre la investigación cuando sea necesario, sin tener que esperar a que la duración de la medida haya finalizado. Además, los investigadores han de mantener informado al Instructor, sea cuando éste determine, sea cuando se interese cualquier nuevo aspecto con respecto a la medida ya acordada, o bien cuando se le ponga fin.

En todos estos supuestos, el art. 588 bis f) LECrim exige aportar un *«informe detallado del resultado de la medida»,* así como una explicación de *«las razones que justifiquen la continuación de la misma»*. La petición de prórroga, y el informe sobre su pertinencia, deben presentarse ante el Juzgado con tiempo suficiente para remitirlo al Ministerio Fiscal para, que si lo estima oportuno informe sobre ella (no es preceptivo su informe en estos casos[204]), así como para que por parte del Juez instructor se pueda dictar la resolución antes de que expire el plazo contenido en la resolución, cosa que sucedería de no acordarse una nueva prórroga, o de hacerse en fecha posterior a su expiración.

El Juez cuenta con un plazo de dos días -cuarenta y ocho horas- (sujeto a lógica ampliación en caso de necesitar mayor aclaración o complemento al oficio donde se solicita la prórroga) para dictar la resolución ampliatoria. Si se pasara el plazo de prórroga y hubiera decaído la vigencia de la medida,

[203] Resulta bastante común en el práctica policial, sobre todo durante la práctica de diligencias de intervención, grabación y escucha telefónica, que en los casos en que la intervención de un teléfono no da resultado, los propios investigadores insten el cese de la escucha, en otras ocasiones, aunque lo solicitan, informan de que el mismo no ha dado resultado y no han continuado con la diligencia.

[204] Pese a no ser preceptivo, la Circular de la Fiscalía General del Estado 1/2019 alerta a los Fiscales para que informen sobre ella. Pág.36.

habría que volver a realizar una nueva solicitud para que se acuerde la diligencia, y no estaríamos propiamente ante una prórroga.

El art. 588 bis f) LECrim apartado 3, establece que el plazo de prórroga de la medida comienza a contar desde la expiración del plazo concedido por el auto inicial o por el último que haya acordado la prórroga de la medida. Por lo tanto, no ha de partirse de la fecha del nuevo auto para computar el plazo de prórroga concedido, sino desde la fecha del auto que es objeto de prórroga.

3.3.2. Información obtenida en procedimientos distintos y hallazgos causales.

En toda investigación criminal es posible que, tras analizar datos o realizar diligencias, se descubra la posible comisión de un delito que inicialmente no estaba siendo objeto de investigación. También cabe que se concluya que el presunto responsable es distinto al sospechoso inicial, o se desvele la participación de un sujeto que no estaba siendo investigado.

La investigación es un proceso en constante evolución, y su desarrollo puede aconsejar que se acumulen los nuevos datos a la causa principal y seguir con ella, o bien se necesite abrir una nueva causa. En este segundo caso se tiene que trasladar esta información de un procedimiento a otro. El traslado de información de un proceso a otro, información que además sirva para que dentro del mismo se incluya un nuevo delito conexo, o se inicie un nuevo procedimiento a instruir, son situaciones, que la doctrina califica de *«auténtica cesión de información»*[205].

El problema que se provoca por esta situación de obtención de nueva información se ciñe al modo en que se ha producido la obtención de los datos, pues algunos de ellos pudieron recabarse empleando una diligencia de limitación de un derecho fundamental, que pasó por el debido control judicial, pero que nunca fue el mismo objeto que el que permitió conocer los nuevos datos obtenidos. En el trascurso de aquella diligencia pudieron llegar datos a la investigación sobre hechos que no se conocían, o sobre personas que no han resultado sospechosas. En suma, como los datos pueden provenir de una diligencia que bien fue acordada para otra finalidad, o para otra

[205] Cfr. VELASCO NÚÑEZ, Eloy. "Investigación tecnológica de delitos: disposiciones comunes e interceptaciones telefónicas y telemáticas". Ponencias de formación. Jornadas de 10 de marzo de 2016 tituladas "Jornadas de especialistas en criminalidad informática". Pág. 10. Texto contenido en el enlace web de la página de el Ministerio Fiscal de España: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20Velasco%20Nuñez,%20Eloy.pdf?idFile=7b2fdf75-4a93-41bd-9adc-fe3042c95cc0. En dicha ponencia se ponen ejemplos muy destacados para diferenciar el uso de los hallazgos en procedimientos distintos de aquél en el que se hubiere producido el hallazgo causal, haciendo un análisis de lo que considera una completa habilitación legal para efectuarlo desde la entrada en vigor del art. 588 bis h). Para mayor abundamiento, la cesión de datos en el marco de las investigaciones penales ha sido desarrolado en Vid. COLOMER HERNÁNDEZ, Ignacio (Dir). *Cesión de datos personales y evidencias entre procesos penales y procedimientos administrativos sancionadores y tributarios*. Aranzadi. Pamplona. 2017.

persona distinta de las que finalmente termina afectando, o se terminan ofreciendo nuevos datos que dan origen a una nueva actuación penal, se plantea la validez de este aspecto.

La doctrina ha definido el hallazgo casual como la *«situación en la que habiendo obtenido la correspondiente autorización judicial para la practica de una diligencia que afecta a los derechos fundamentales del sujeto investigado, con motivo de la persecución de unas conductas concretas y determinadas, aparecen fuentes de prueba relativas a otro u otros delitos distintos de los que no se tenía noticia con anterioridad»*[206].

El concepto debe ponerse en relación con el de hecho nuevo, que se define como la «*aparición de esos hechos delictivos nuevos durante la ejecución de una diligencia de investigación restrictiva de derechos fundamentales»*[207].

La nota común a ambos conceptos es que en ellos hay una diligencia limitadora de derechos que ha posibilitado obtener una nueva fuente de prueba o bien conocer un hecho ilícito distinto.

La doctrina ha cuestionado el alcance que deben tener estos nuevos datos obtenidos durante el desarrollo de las diligencias de investigación, en particular la de entrada y registro en domicilio, así como en la consistente en la intervención de las comunicaciones, pues *«el problema ... es el relativo a determinar si las evidencias probatorias así obtenidas son susceptibles de ser incorporadas al proceso o proceso distinto, y, en consecuencia, si a ese resultado imprevisto se le puede dotar de valor probatorio, o si, por el contrario, ha de ser rechazado»*[208].

Estos interrogantes que se hacían sobre determinadas diligencias pueden extenderse, en la actualidad, a las variadas diligencias investigadoras que limitan los derechos del art. 18 CE, y por lo tanto también a las de acceso y registro de datos.

El examen de un dispositivo de almacenamiento masivo de información, o durante la práctica de una diligencia de intervención remota de un equipo informático, admite que se produzca la aparición de datos, documentos, o rastros de comunicaciones electrónicas ya finalizadas, en las que los investigadores podrán encontrar tanto indicios de la comisión de nuevos delitos, como

---

[206] Cfr. ECHARRI CASI, Fermín Javier. «Prueba ilícita: conexión de antijuridicidad y hallazgos casuales*» en Revista del Poder Judicial* nº 69, 2003, p. 22. En los mismos términos, Cfr. NADAL GÓMEZ, Irene. «El régimen de los hallazgos casuales en la Ley 13/2015, de modificación de la LECrim». *Revista General de Derecho Procesal*. nº 40. 2016. Pág. 7.

[207] Cfr. ÁLVAREZ DE NEYRA KAPPLER, Susana.«Los descubrimientos causales en el ámbito de una investigación penal (con especial relevancia a las diligencias de entrada y registro en domicilio)», *Revista internacional de estudios de Dereceho Procesal y Arbitraje* . nº2 , año 2011. Pág. 4. En los mismos términos, Cfr. NADAL GÓMEZ. Op. Cit. Pág. 8.

[208] Cfr. GARCÍA SAN MARTÍN, Jerónimo. "El hallazgo casual o descubrimiento ocasional en el ámbito de la investigación penal" *La Ley Penal*, Nº 109, Julio-Agosto 2014. LA LEY 4917/2014. Pág. 2.

circunstancias que respalden la posibilidad de que existan más personas relacionadas con el hecho investigado, que no siendo identificadas de forma inicial, ahora sí que resulten determinadas.

La conclusión de la doctrina es favorable a que la regla sobre los hallazgos casuales se aplique a las nuevas diligencias de investigación. Si el derecho que estas diligencias afectan es el mismo que el que se veía afectado en las diligencias de intervención de comunicaciones o registros domiciliarios, la extensión de estas categorías conceptuales a las nuevas diligencias es posible [209].

En suma, si los nuevos hechos delictivos son susceptibles de ser considerados como delitos conexos, tal y como los regula el actual art. 17 LECrim[210], los datos que hayan sido tenidos en cuenta para la averiguar un hecho delictivo conectado con el inicialmente investigado, no presentan problemas para servir de acreditación de otro con el que guarden relación de conexidad. La ventaja de la conexidad dentro del proceso implica, siguiendo la doctrina que *«el hecho de que se tramiten en un solo proceso y en la misma sentencia podrá facilitar ..... la utilización probatoria de materiales obtenidos indistintamente en la investigación de cualquiera de estos delitos en el seno del mismo procedimiento»*[211].

---

[209] Vid. NADAL GÓMEZ. Op. cit. Página. 52. Dice la autora textualmente que *« Las diligencias en las que con mayor probabilidad pueden ocasionarse hallazgos casuales son las de captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización; el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos. »*

[210] Este precepto ha sido modificado por la Ley 41/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento criminal para la agilización de la justicia penal el fortalecimiento de las garantías procesales. El artículo 17 LEcrim, en su nueva redacción supone una clara manifestación de la voluntad del legislador por acelerar en la medida de lo posible los procesos penales, pues se pretende, en palabras de la Exposición de Motivos la «*racionalización de los criterios de conformación del objeto del proceso, con el fin de que tengan el contenido más adecuado para su rápida y eficaz sustanciación. Con ello se pretende evitar el automatismo en la acumulación de causas y la elefantiasis procesal que se pone de manifiesto en los denominados macroprocesos»*. Por ello, continúa la Exposición de Motivos indicando que «*La novedad de la reforma consiste en establecer que la simple analogía o relación entre sí no constituye una causa de conexión y solo se justifica la acumulación cuando, a instancia del Ministerio Fiscal, en su condición de defensor de la legalidad y del interés público, el juez lo considere más conveniente para el esclarecimiento de los hechos y la determinación de las responsabilidades procedentes, salvo que suponga excesiva complejidad o dilación para el proceso, y siempre que con ello no se altere la competencia. Así, además, se evitará el frecuente trasiego de causas entre distintos juzgados a la búsqueda del que deba conocer del asunto por una simple coincidencia de la persona a la que se atribuyen distintos delitos»*. Ante esta situación, la redacción del art. 17 LEcrim, dispone que son delitos conexos: *«1.º Los cometidos por dos o más personas reunidas, 2.º Los cometidos por dos o más personas en distintos lugares o tiempos si hubiera precedido concierto para ello, 3.º Los cometidos como medio para perpetrar otros o facilitar su ejecución, 4.º Los cometidos para procurar la impunidad de otros delitos; 5.º Los delitos de favorecimiento real y personal y el blanqueo de capitales respecto al delito antecedente y 6.º Los cometidos por diversas personas cuando se ocasionen lesiones o daños recíprocos».* En consecuencia, esto supondrá que se dejará de lado la regla general de que cada delito debe constituir una sola causa y «*serán investigados y enjuiciados en la misma causa cuando la investigación y la prueba en conjunto de los hechos resulten convenientes para su esclarecimiento y para la determinación de las responsabilidades procedentes salvo que suponga excesiva complejidad o dilación para el proceso»*. Por su parte, el apartado tres del precepto, sienta otra excepción a esta regla general en los casos previsto en ella, cuando dispone que los «*delitos que no sean conexos pero hayan sido cometidos por la misma persona y tengan analogía o relación entre sí, cuando sean de la competencia del mismo órgano judicial, podrán ser enjuiciados en la misma causa, a instancia del Ministerio Fiscal, si la investigación y la prueba en conjunto de los hechos resultan convenientes para su esclarecimiento y para la determinación de las responsabilidades procedentes, salvo que suponga excesiva complejidad o dilación para el proceso»*.

[211] Cfr. NADAL GÓMEZ. Op. cit. Página. 20.

Por otro lado, si no son delitos conexos, será necesario valorar si la diligencia practicada para averiguar un concreto delito, y que ha concluido con indicios de la comisión de nuevos hechos ilícitos, que no eran los inicialmente investigados, o con la existencia de nuevos posibles responsables penales, es procedente[212]. Esta procedencia concurre cuando la medida acordada se ajusta a los parámetros legales, jurisprudenciales y fácticos necesarios para llevarla a cabo, lo que, de darse supone respaldar la legitimidad de la medida.

En otras palabras, se exige que tanto la resolución judicial que acordó la práctica de la diligencia de investigación durante la que se encontraron los hallazgos, estuviera dictada conforme a los parámetros legales, como que, la diligencia derivada de la misma, y que sirve para ahondar en tales hallazgos, también exista y se ajuste a los mismos parámetros de legalidad[213].

Hay autores que consideran que cuando no se esté ante delitos conexos se deberá iniciar una nueva instrucción penal diferenciada e independiente *«lo que…exigiría la apertura de un nuevo proceso y, en su caso, una nueva autorización judicial para realizar la concreta diligencia»*[214].

El Tribunal Supremo ha elaborado su propia doctrina, que es favorable a contar con el resultado de estas diligencias, pero siendo escrupuloso a la hora de exigir garantías en orden a su validez[215].

---

[212] Cfr. NADAL GÓMEZ. Op. cit. Página. 21. La autora sostiene que resulta totalmente necesario acreditar *«la legitimidad de la medida en que se produjo la injerencia»*.

[213] Cfr. NADAL GÓMEZ. Op. Cit. Pág. 24. *«.. la posible utilización de tales hallazgos está supeditada a que la medida en la que se originó fuera legítima con especial referencia al escrito de solicitud, a la resolución por la que se autoriza y se prorroga le medida de origen. Y mas allá del propio descubrimiento, una vez producido éste, requiere que la diligencia en la que el mismo se investigue sea autorizada por el juez competente…. . Sólo cuando se haya cumplido con todas estas exigencias de legalidad ordinaria y constitucional, los hallazgos casuales podrán desplegar toda la eficacia que la nueva normativa les reconoce* »

[214] Cfr. ÁLVAREZ DE NEYRA KAPPLER, Susana. «Los descubrimientos casuales en el marco de una investigación penal (con especial referencia a las diligencias de entrada y registro en domicilio». *Revista internacional de Estudios de derecho procesal y arbitraje*. Septiembre de 2011. Página 6. http://www.riedpa.com/COMU/documentos/RIEDPA21101.pdf.

[215] La STS 991/2016, de 12 de enero de 2017. Ponente: Don Alberto Gumersindo Jorge Barreiro, recoge la doctrina del Tribunal Supremo sobre esta particular institución. Por citar alguna de reciente redacción, la STS 400/2017, de 1 de junio. Ponente: Don Juan Saavedra Ruíz, página 11 y siguientes, recuerda la doctrina aludida, manteniendo que *«el que se estén investigando unos hechos delictivos no impide la persecución de cualesquiera otros distintos que sean descubiertos por casualidad al investigar aquéllos, pues los funcionarios de Policía tienen el deber de poner en conocimiento de la autoridad penal competente los delitos de que tuviera conocimiento, practicando incluso las diligencias de prevención..* ». Sigue sosteniendo la sentencia que «*cuando se trata de investigaciones realizadas mediante intervenciones telefónicas, entre los requisitos que deben ser observados se encuentra el de la especialidad de la medida , en el sentido de que la intervención debe de estar orientada hacia la investigación de un delito concreto, sin que sean lícitas las observaciones encaminadas a una prospección sobre la conducta de una persona en general. Lo que no excluye que los hallazgos casuales sugerentes de la posible comisión de otros delitos distintos no sean válidos, sino que la continuidad en la investigación de ese hecho delictivo nuevo requiere de una renovada autorización judicial (en este sentido, entre otras, SSTS 468/2012, de 11 de junio ; 157/2014, de 5 de marzo ; 425/2014, de 28 de mayo ; 499/2014, de 17 de junio)».* El núcleo de dicha doctrina lo encontramos en el texto de la sentencia cuando afirma que «e*l hallazgo casual, es decir, el elemento probatorio novedoso que no está inicialmente abarcado por el principio de especialidad, puede ser utilizado en el propio o distinto procedimiento, bien por tratarse de un delito flagrante o bien por razones de conexidad procesal, siempre que, advertido el hallazgo, el juez resuelva expresamente continuar con la investigación para el esclarecimiento de ese nuevo delito, ante la existencia de razones basadas en los principios de proporcionalidad e idoneidad. El hallazgo no solamente se proyecta hacia el futuro, como en el caso de unas*

Este parecer ha sido desarrollado por algún Acuerdo de la Sala Segunda del TS relativo al inicio de nuevas actuaciones penales derivadas de datos obtenidos en otros procesos judiciales[216].

El legislador, finalmente, ha optado en la reforma de 2015, por cristalizar en norma jurídica positiva, y elevar por tanto a rango de ley, el contenido de dicha jurisprudencia.

La nueva regulación de esta materia está en el art. 579 bis LECrim, que es la que fija cómo ha de llevarse a cabo el tratamiento de los datos que se han obtenido dentro de otro proceso, o bien los que se consiguieron de manera casual. Es una norma que se aplica a las diligencias de investigación reguladas en los Capítulos III, V, VI, VII, VIII y IX, por expreso mandato del art. 588 bis i LECrim.

El legislador parte de la posibilidad de que durante la práctica de alguna de las diligencias de investigación tecnológica se obtengan datos de la comisión de un delito distinto al investigado, o bien se encuentren los datos de una nueva persona que deba ser sometida a investigación penal por su relación con los hechos, o bien que ambas circunstancias se produzcan a la vez. El art. 579 bis LECrim dedica los dos primeros párrafos a la regulación de la investigación de delitos realizada a partir de datos obtenidos en procesos distintos, mientras que el párrafo tercero contiene la regulación procesal del denominado hallazgo casual[217].

---

intervenciones telefónicas en donde resultan indicios de la comisión de otros delitos diferentes a los investigados, sino que también puede producirse hacia el pasado, como cuando en el curso de un registro domiciliario aparecen evidencias de otros ilícitos, o cuando las intervenciones telefónicas pueden arrojar datos sustanciosos acerca de la participación de los comunicantes en hechos no inicialmente investigados por esa vía, con tal que, como hemos dicho, tal línea de investigación sea puesta de manifiesto ante el juez, y éste, valorando los intereses en juego, acceda a su incorporación al proceso, conjugando un elemental principio de proporcionalidad. Se trata, en suma, de aquellos descubrimientos casuales que pueden aportar luz para el esclarecimiento de los hechos de carácter novedoso (puesto que permanecían ocultos), y que han de ser investigados, siempre que la autoridad judicial pondere su importancia, salvaguarde el principio de especialidad y justifique su necesidad y proporcionalidad». Por último cabe reseñar que la propia sentencia recoge otro de las doctrinas que ha servido al Alto Tribunal a los efectos de justificar la procedencia de la diligencia de investigación que inicialmente acordada para investigar un hecho, sirve para iniciar la investigación de otro distinto de aquél, siendo en este caso la Doctrina de la flagrancia, según la cual, dice la sentencia que "«l*a Sala, no sin ciertas oscilaciones, admitió la validez de la diligencia cuando, aunque el registro se dirigiera a la investigación de un delito específico, se encontraran efectos o instrumentos de otro que pudiera entenderse como delito flagrante. La teoría de la flagrancia ha sido, pues, una de las manejadas para dar cobertura a los hallazgos casuales, y también la de la regla de la conexidad de los arts. 17.5 y 300 LECrim , teniendo en cuenta que no hay novación del objeto de la investigación sino simplemente " adición"» .*

[216] Esta cuestión fue objeto del Acuerdo de Pleno de la Sala segunda del Tribunal Supremo de 26 de mayo de 2009, a cuyo tenor *«en los procesos incoados a raíz de la deducción de testimonios de una causa principal, la simple alegación de que el acto jurisdiccional limitativo del derecho al secreto de las comunicaciones es nulo, porque no hay constancia legítima de las resoluciones antecedentes, no debe implicar sin más la nulidad. En tales casos, cuando la validez de un medio probatorio dependa de la legitimidad de la obtención de fuentes de prueba en otro procedimiento, si el interesado impugna en la instancia la legitimidad de aquel medio de prueba, la parte que lo propuso deberá justificar de forma contradictoria la legitimidad cuestionada. Pero, si, conocido el origen de un medio de prueba propuesto en un procedimiento, no se promueve dicho debate, no podrá suscitarse en ulteriores instancias la cuestión de la falta de constancia en ese procedimiento de las circunstancias concurrentes en otro relativas al modo de obtención de las fuentes de aquella prueba».* Sirva como sentencia ejemplificativa de la aplicación del contenido de este Acuerdo el que se contiene en la STS 737/2009 de 6 de julio. Ponente: Don Joaquín Jiménez García.

[217] Vid. LÓPEZ JIMÉNEZ, Raquel «Régimen jurídico de los datos personales obtenidos en los descubrimientos casuales durante la investigación de los delitos» en COLOMER HERNÁNDEZ, Ignacio. (Dir) *Cesión de datos personales y evidencias entre procesos penales y procedimeintos administrativos sancionadores o tributarios* .

El párrafo primero del 579 bis LECrim permite que los datos obtenidos en un procedimiento, y que tengan la autonomía suficiente como para dar origen a una nueva investigación penal, puedan servir tanto de medio de investigación, o bien como prueba, en otro proceso penal distinto. Estos datos tendrían la función de ser fuente de prueba en otro proceso penal, o bien puede servir como medio de investigación de un hecho penal.

El párrafo segundo regula el procedimiento que debe seguirse para que esto suceda y puedan hacerse valer tales datos en un proceso distinto[218]. Para que se produzca dicha validez se ha de expedir un testimonio de aquéllos folios de las actuaciones en las que constan dichas medidas (lo que realizará el Letrado de la Administración de justicia), y con ello se consigue acreditar el contenido de las diligencias iniciales practicadas, de esta manera se dota de garantía al nuevo proceso que se abre, porque en éste constarán todos los datos encontrados.

La finalidad de evitar dejar como indeterminados los datos que pueden llegar a constituir el origen de una nueva causa penal, es la que exige la inclusión. Para lograr una transparencia total en el origen de los datos que se vayan a usar para abrir un nuevo procedimiento penal, el art. 579 bis 2 LECrim enumera lo que considera como "*antecedentes indispensables*", incluyendo entre ellos la petición inicial de solicitud de diligencia, también la de la resolución judicial que finalmente acordó que se ejecutase, así como, también, de las diferentes resoluciones que acordaron las sucesivas prórrogas a la medida limitadora de derechos que se hubieran acordado. Esta exigencia legal es claramente conforme con la doctrina de la Sala segunda ya aludida con anterioridad. Por ello, cabe entender que no existe razón alguna para que dichos documentos se vean ampliados más allá de los que la ley estima necesarios para complementar la información legalmente exigida, esto es, para acreditar la legalidad de la injerencia[219].

No hay duda que, la inclusión de todos los antecedentes de la diligencia acordada, permite al investigado hacer efectivo su derecho a la defensa, pues, al estar unidas a las actuaciones todas las

---

Thomson Reuters Aranzadi . Pamplona 2017. Págs. 315 a 343. La autora sostiene acerca del hecho de que en un solo precepto se mezcle la regulación de lo que denomina como *«dos problemas distintos»,* algo criticable, que hubiera sido mejor regulado con la promulgación de un precepto aplicable a cada cuestión, que además fuera de aplicación no sólo a estas diligencias de investigación recogidas en la reforma, sino a todas las demás.

[218] Sobre la validez de los datos obtenidos durante la investigación y su aportación a un proceso judicial distinto, la doctrina ha planteado que la actual regulación, al venir referida, exclusivamente al contenido de los derechos del art 18 CE, deja sin atender otros derechos de rango constitucional que se verían igualmente afectados, por lo que se critica lo insuficiente de la regulación sobre este particular. Vid. AZAUSTRE RUÍZ, Pablo. «Acercamiento al régimen jurídico procesal previsto para la utilización de la información obtenida en un procedimeinto penal distinto» en COLOMER HERNÁNDEZ, Ignacio. (Dir) *Cesión de datos personales y evidencias entre procesos penales y procedimeintos administrativos sancionadores o tributarios* . Thomson Reuters Aranzadi . Pamplona 2017. Págs. 350 y 351

[219] Esta parece ser la línea exigible a la Fiscalía. Así del texto de la Instrucción 2/2017 sobre procesos incoados a raíz de la deducción de testimonio de una causa principal, se recoge en el punto cuarto de sus conclusiones finales que : «*En cuanto a qué deban considerarse testimonios a incorporar, lo serán en cada supuesto concreto todos los testimonios de los particulares necesarios para acreditar la legitimidad de la injerencia»*.

resoluciones mediante las que se obtuvieron los indicios de comisión delictiva, el investigado puede conocer todos estos extremos, puede impugnarlos y defenderse cuestionando la validez de la petición inicial de la diligencia restrictiva de derechos. De hecho, al investigado se le abre, inclusive, la posibilidad de poder examinar si durante la substanciación de la instrucción en el procedimiento penal inicial se dieron todos los requisitos suficientes para garantizar que las prórrogas que, eventualmente, se hayan acordado respetaron los principios jurisprudenciales.

El párrafo tercero del 579 bis LECrim dispone además que la continuación de la medida para la investigación del delito casualmente descubierto habrá de ser acordada por el Juez competente, de acuerdo a dos criterios: atendiendo al marco en que se produjo el hallazgo y la imposibilidad de haber interesado la medida en su momento.

Esto implica que el auto que acuerde la ampliación tendrá que examinar el modo en que se ha producido el hallazgo, si éste ha sido sorpresivo, o, por el contrario, hubiera resultado esperable atendidas las circunstancias del caso, etc. Esto condiciona directamente la constatación del segundo de los criterios para su adopción, pues si no era esperable encontrar los datos localizados, tanto más complicado hubiera resultado para los investigadores solicitar una medida de investigación sobre el particular. En este sentido debe recordarse el papel del Ministerio Fiscal en cuanto a la cuestión[220]. En concreto hay que tener presente que la Instrucción de la FGE 2/2017 sobre procesos incoados a raíz de la deducción de testimonio de una causa principal, ordena a los Fiscales que adopten un papel activo en la salvaguarda de la legalidad de este mecanismo de inicio de una nueva actuación penal, estableciendo su obligación de examen de la causa, recabando los datos y documentos que pudieran faltar en ella, asegurándose su inclusión desde el inicio de la misma.

Para finalizar, el artículo 579 bis, párrafo 3, recoge la eventualidad de que el hallazgo casual suceda en el seno de una causa declarada secreta[221]. En este supuesto es preceptivo que el Juez que tiene

[220] El punto 6 de la Circular de la Fiscalía General del Estado 1/2013, *«sobre pautas en relación con la diligencia de intervención de comunicaciones telefónicas»* ya recogía la doctrina jurisprudencia que hemos tenido ocasión de aludir, proclive a la estimación del hallazgo casual, siempre que se den las debidas garantías, como fórmula de inicio de una nueva línea de investigación o ampliación de la existente, estableciendo que el papel del Fiscal no es otro que el de velar por la legalidad de la medida adoptada.

[221] Los artículos 301 y 302 de la LEcrim, relativos al secreto del sumario, han sido objeto de modificación tras la promulgación de la Ley Orgánica 5/2015, de 27 de abril, por la que se modifican la Ley de Enjuiciamiento Criminal y la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, para transponer la Directiva 2010/64/UE, de 20 de octubre de 2010, relativa al derecho a interpretación y a traducción en los procesos penales y la Directiva 2012/13/UE, de 22 de mayo de 2012, relativa al derecho a la información en los procesos penales. La Exposición de Motivos, en su apartado IV, considera el secreto una excepción del derecho de acceso del investigado al contenido del procedimiento. Determina el artículo 302 que *«podrá el Juez de Instrucción, a propuesta del Ministerio Fiscal, de cualquiera de las partes personadas o de oficio, declararlo, mediante auto, total o parcialmente secreto para todas las partes personadas, por tiempo no superior a un mes cuando resulte necesario para: a) evitar un riesgo grave para la vida, libertad o integridad física de otra persona; o b) prevenir una situación que pueda comprometer de forma grave el resultado de la investigación o del proceso. El secreto del sumario deberá alzarse necesariamente con al menos diez días de antelación a la conclusión del sumario»*.

declarada secreta la causa tenga que comunicar el fin de esta situación al que instruye la otra, para así respetar el correcto ejercicio del derecho de defensa que asiste a todo investigado.

El secreto de la causa impide que el investigado pueda tener a su disposición todos los elementos obrantes en ella, en especial los referentes a su presunta participación[222], razón que motiva que para una más adecuada y eficaz protección de su derecho a la defensa se suelan acoger a su derecho a no declarar, y pospongan su declaración hasta que conozcan todos los extremos del procedimiento.

La declaración de secreto exige también una resolución especialmente motivada, siendo una cuestión que se deja al control judicial y que se arbitra respetándose el contenido del art. 302 LECrim.

La aparición de hallazgos casuales no impide que la causa continúe siendo secreta. En todo caso si tal hallazgo determina la necesidad de que se aperture una nueva, por resultar exigible al tratarse de una nueva noticia *criminis*, y no de un hecho conexo al investigado, el Juez tiene que poner de manifiesto que la causa de la que procede este nuevo dato se encuentra declarada secreta. Dicho Instructor está obligado a comunicar al Juzgado que pudiera estar instruyendo de la nueva causa el cese del secreto cuando suceda. Esta comunicación conllevará, que en esta segunda causa también se eleve esta restricción de acceso, cuando concurran las razones procesales para hacerlo, y puedan efectuarse las funciones de las defensas con completa normalidad. En este sentido, no se debe olvidar que la instrucción de cada causa es autónoma, lo que implica que las razones que motiven el levantamiento del secreto de la causa no pueden obedecer únicamente al contenido del art. 579 bis LECrim, sino también al propio objeto de investigación.

4. La afectación a terceros por la adopción de la medida acordada.

[222] La Circular de la Fiscalía General del Estado 3/2018 de 1 de junio sobre el derecho de información de los investigados en los procesos penales realiza un estudio muy interesante de los derechos tanto del detenido como del investigado a acceder a las actuaciones y a conocer las razones de su situación a la luz de distintas normas europeas y algunos pronunciamientos del TC. En suma cabe decir que cada vez es más amplio el acervo de derechos que en relación a la información de elementos que obran en las actuaciones conciernen al afectado por el proceso. En especial en el caso de actuaciones bajo secreto y puesto en relación con la posible comparecencia para determinar la prisión provisional prevista en el art. 505 LECrim determina la conclusión 13, página 61, a cuyo tenor: "«*13ª En los casos en los que estuviera declarado el secreto de las actuaciones, los Sres. Fiscales deberán también velar por que se le facilite al privado de libertad el acceso a aquellos elementos de las actuaciones que resulten esenciales para impugnar su privación de libertad con carácter previo a la comparecencia prevista en el art. 505 LECrim y en los términos expuestos en la presente Circular. El acceso debe producirse de forma efectiva, mediante exhibición, entrega de copia o cualquier otro método que, garantizando la integridad de las actuaciones, permita al investigado conocer y comprobar por sí, o a través de su letrado, los elementos esenciales para impugnar la privación de libertad».*

Uno de los principios rectores para acordar una diligencia de investigación, en concreto el principio de especialidad, obliga a toda investigación criminal a que guarde relación con unos hechos concretos, atribuibles de forma indiciaria a una persona determinada; el investigado. La instrucción no puede apartarse en ningún momento de este sujeto, salvo que ello sea para sobreseer las actuaciones.

La investigación versa sobre la relación que este investigado guarda con la comisión de hechos con trascendencia penal. La relación del investigado con los hechos no puede ser cualquiera, sino que su conexión con la comisión de los hechos sólo podrá concretarse en alguna de las formas de participación previstas en el Código Penal. El hecho de ser declarado investigado refuerza el despliegue de los derechos fundamentales referentes a la defensa, que deben ser respetados escrupulosamente en el transcurso de esta investigación.

La reacción que ofrece el ordenamiento jurídico ante situaciones que obvien, limiten o simplemente inapliquen esa necesaria observancia de los derechos fundamentales, es la de dejar expuesta la instrucción penal a una evidente nulidad de actuaciones[223], extremo que ha sido muy estudiado por la jurisprudencia[224].

---

[223] Dispone el art. 11.1 de la Ley Orgánica 6/1985 de 1 de julio, en su art. 11.1 que «*en todo tipo de procedimiento se respetarán las reglas de la buena fe. No surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades fundamentales»*. A senso contrario, cualquier prueba que se haya obtenido mediante la violación de alguno de estos derechos quedará viciada de nulidad de pleno derecho y no podrá surtir eficacia en el proceso penal. En todo caso debe tenerse presente el contenido de la STS 116/2017, de 23 de febrero. Ponente: D. Manuel Marchena Gómez. Dicha sentencia, dictada con ocasión de un recurso de casación interpuesto por la representación del condenado como autor de dos delitos contra la Hacienda Pública, instruído al amparo de la información obtenida por la AEAT de la llamada "lista Falciani", viene a matizar el contenido de la doctrina sobre el art. 11.1 LOPJ. Conforme a esta matización es posible admitir, en algunos casos, las pruebas con trascendencia penal obtenidas por particulares y no por el Estado o sus agentes, y que las mismas surtan efectos en el proceso penal, incluso aunque vulneren derechos fundamentales. Esta idea se ve inmediatamente matizada en el sentido de que ha de verse afectado algún aspecto accesorio del derecho fundamental, porque si se limita o vulnera el nucleo esencial del derecho, tampoco debería admitirse dicha prueba.En todo caso es imprescindible un juicio de ponderación y proporcionalidad.

[224] Por citar jurisprudencia reciente, cabe reseñar la STS 106/2017, de 21 de febrero. Ponente: D. Antonio del Moral Garcia. La sentencia recoge la doctrina del TC sobre la nulidad de actuaciones que concurre cuando no se evita la investigación prospectiva. Se dice en la citada sentencia: «*Se trata, por consiguiente, de determinar si en el momento de pedir y adoptar la medida de intervención se pusieron de manifiesto ante el Juez, y se tomaron en consideración por éste datos objetivos que permitieran precisar que dicha línea era utilizada por las personas sospechosas de la comisión del delito o de quienes con ella se relacionaban, y que, por lo tanto, no se trataba de una investigación meramente prospectiva, pues el secreto de las comunicaciones no puede ser desvelado para satisfacer la necesidad genérica de prevenir o descubrir delitos o para despejar las sospechas sin base objetiva que surjan en los encargados de la investigación, ya que de otro modo se desvanecería la garantía constitucional (por todas, SSTC 49/1999, de 5 de abril, FJ 8 ; 166/1999, de 27 de septiembre, FJ 8 ; 171/1999, de 27 de septiembre, FJ 8 ; 167/2002, de 18 de septiembre, FJ 2 ; 259/2005, de 24 de octubre, FJ 2 ; 253/2006, de 11 de septiembre , FJ 2)*". Sigue diciendo la sentencia que "*el Tribunal ha considerado insuficiente la mera afirmación de la existencia de una investigación previa, sin especificar en qué consiste, ni cuál ha sido su resultado por muy provisional que éste pueda ser, afirmando también que la concreción del delito que se investiga, las personas a investigar, los teléfonos a intervenir y el plazo de intervención no pueden suplir la carencia fundamental de la expresión de los elementos objetivos indiciarios que pudieran servir de soporte a la investigación, ni la falta de esos indispensables datos pueda ser justificada a posteriori por el éxito de la investigación misma (SSTC 299/2000, de 11 de diciembre, FJ 5 ; 138/2001, de 18 de junio, FJ 4 ; 167/2002, de 18 de septiembre, FJ 3 ; 165/2005, de 20 de junio, FJ 5 ; 259/2005, de 24 de octubre, FJ 4 ; 253/2006, de 11 de septiembre ,*

La investigación penal es una actividad flexible, viva y sujeta a nuevos hechos que puedan aparecer en la búsqueda de la realidad material. Y aunque el contenido del proceso debe estar referido a la actuación u omisión de una persona concreta, que es tenida como indiciariamente responsable de los hechos ilícitos, ello no impide que durante el transcurso del acto delictivo concurra con el inicial investigado, de alguna forma, el comportamiento de otro u otros sujetos. La participación de terceros puede ser muy diversa, y puede servir para obtener datos que afiancen la investigación iniciada.

La relación de una tercera persona en los hechos no siempre ha de conllevar responsabilidad criminal, y por lo tanto no tiene porqué ocupar el papel de investigado. En todo caso, el hecho de no ser el investigado en la causa penal, no priva a este tercero de los derechos fundamentales que le asisten. Por ejemplo pueden ser terceros desde testigos de los hechos hasta cualquier persona que actúa con el investigado, a sabiendas o no de sus actos.

Las personas que se relacionan con el investigado de modo diario también pueden aparecer en la causa[225]. El contacto con el investigado, voluntario o no, puede afectar al contenido de sus propios derechos, lo que se prolongará en el tiempo a medida que de la relación que investigado y tercero mantienen, se obtengan datos útiles para la investigación.

El tercero no tiene que colaborar necesariamente con el investigado en la comisión del hecho antijurídico ejecutado, y puede ignorar completamente la acción penal llevada a cabo por éste. El tercero se ha de ver como un sujeto cuyas actividades, relacionadas con las del investigado, pueden servir de fuente de prueba de hechos cometidos por el investigado.

Estas interrelaciones del investigado con terceros conducen a cuestionarse cómo debe tratarse la información en la que intervienen o se afectan a esos terceros. En especial, también hay que hacerlo cuando la información se obtiene mediante alguna diligencia del Título VIII de la LECrim.

La legislación procesal anterior a la reforma era parca, cuando no completamente ajena, a la hora de tener en cuenta el papel de la presencia de terceros, entendidos como elementos de la investigación. Esta carencia era suplida por la doctrina del Tribunal Constitucional y del Tribunal Supremo, que arbitraba las soluciones ante las diversas situaciones de la práctica. En este sentido, por ejemplo, se

---

FJ 4)». Pág. 6 y 7. También cabe citar sobre el mismo asunto la STS 841/2016 de 8 de noviembre. Ponente: Don Juan Ramón Verdugo Gómez de la Torre.

[225] A título de ejemplo, pensemos en todas esas personas con las que el investigado intercambia conversaciones telefónicas, o mails, en la que se exponen datos que, debidamente relacionados entre sí, puedan ser de interés en la causa. Puede que, de manera involuntaria, se determine un lugar donde haya podido estar el investigado, o saber con qué persona estuvo, etc. Puede tratarse de personas con las que el investigado tiene una relación de confianza que le permite tomarle prestado algún objeto de uso cotidiano, como un teléfono, un ordenador, una tablet, etc, que se puede usar para perpetar el delito. Estas personas pueden ser el abogado de confianza, un médico, la propia pareja, los hijos, amigos, etc.

distinguía entre la intervención de comunicaciones de la víctima [226], o la intervención de comunicaciones de terceros que pudieran guardar o no relación con los hechos[227], etc.

La nueva regulación procesal, tras la reforma de 2015 de la LECrim, si contempla estas situaciones. De hecho, se ha insertado un precepto que, con carácter general, regula como ha de tratarse la afectación de terceros en la práctica de diligencias. El art. 588 bis h) LECrim es la disposición general sobre esta materia, y se completa con el contenido que cada diligencia de investigación en particular contenga sobre esa cuestión.

El papel que realiza un tercero puede variar para cada tipo de diligencia de investigación, siendo más intensa en unas que en otras[228].

En el caso concreto de la diligencia de acceso y registro de un dispositivo de almacenamiento masivo de información, también se pueden afectar a los derechos de terceros, casi como cualquier otra. Puesto que, en ocasiones, es posible que la información que esté contenida dentro del dispositivo a registrar sea referente a personas distintas al investigado: fotografías, vídeos, documentos diversos, referidos a otras personas distintas del investigado, o incluso, cabe la

[226] STS 393/2015, de 12 de junio. Ponente: D. Juan Maza Martín, o la SAP de Pontevedra 5/2006, de 10 de mayo. Ponente: D. Manuel Almenar Belenguer. Ambas sentencias estiman que es posible dentro de la instrucción de la causa admitir la intervención de las comunicaciones de la propia víctima. La mencionada sentencia del Tribunal Supremo realiza además una justificación de la medida estimando que en base a la aplicación del principio de proporcionalidad se considera una medida adecuada.

[227] En esta materia cabe reseñar el contenido de la STS 1947/2002, de 29 de diciembre. Ponente: D. Joaquín Jiménez García. En la sentencia se analiza la autorización que en su momento fue dada para intervenir el teléfono de los padres del recurrente (página 6). El Tribunal analiza la procedencia de dicha intervención admitiéndola y considerándola ajustada a derecho por considerar que se había realizado una adecuada ponderación y valoración judicial acerca de su procedencia, acudiendo a los tradicionales criterios y principios necesarios para su admisibilidad. Más elocuente y explícita sobre la procedencia de la intervención de la comunicación de terceros es la STS 1008/2013, de 8 de enero de 2014. Ponente: Don Cándido Conde-Pumpido Tourón. En dicha sentencia se emplea la alocución «ampliación subjetiva» como aquélla que denomina la intervención de comunicaciones de terceros que en este caso guardaban cierta relación con los hechos; el texto de la sentencia dice que «*Cuando, como sucede en este caso, se trata de una extensión personal, es decir de una ampliación subjetiva, extendiendo la intervención a otros sujetos pasivos que tienen vínculos de conexión con el delito investigado, solo es necesario ponderar los indicios objetivos de la conexión de los nuevos sujetos con dicho delito, partiendo de la base de que la necesidad y proporcionalidad de la utilización de la medida para la investigación de los hechos delictivos de que se trate ya está fundamentada en la resolución inicial.*
Y esta conexión puede venir determinada precisamente por la naturaleza de las conversaciones telefónicas que los ya investigados sostienen con el titular de la nueva línea cuya intervención se solicita. Es decir, no es necesario en estas ampliaciones subjetivas que se justifique nuevamente la concurrencia de indicios de que se está realizando una actividad delictiva, y de la proporcionalidad y necesidad de la medida, que ya está acordada en el procedimiento, sino exclusivamente de la conexión del titular de la nueva línea cuya intervención se solicita, con el delito que ya se está investigando». Como puede verse se trata en este caso, como se ha dicho de la intervención de comunicaciones de terceros que guardan relación directa con los hechos solo requiere la ponderación de indicios que hagan suponer que estos nuevos sujetos guardan relación con los hechos que están siendo investigados, sin que sea necesaria la ponderación habitual sobre la proporcionalidad de la medida, lo cual ya se dio en el origen del proceso. De aquí debe deducirse que en el caso en que no estuviera implicado, si que debe realizarse tal ponderación, como de hecho se aludía en la primera de las sentencias mencionadas en esta nota.

[228] Por ejemplo, en la intervención de comunicaciones se exige siempre y en todo caso la presencia de un emisor y de un receptor, y como cualquiera de los dos puede ser un tercero a los efectos de la investigación, es lógico que la LECrim se detenga más en el papel de un tercero en la diligencia de intervención de las comunicaciones, que en otras diligencias en las que no predomina tanto ese intercambio, o la concurrencia de más de una persona.

posibilidad de que los datos pertenezcan a distintos usuarios de un dispositivo compartido por varias personas siendo una de ellas el investigado. En todos estos casos hay datos que pertenecen a terceras personas, que incluso pueden estar relacionados con el investigado, que deben encontrar la protección adecuada dentro del proceso penal.

En la otra diligencia de control y acceso remoto a un equipo informático, es posible también que haya terceros afectados. Pues, al tratarse de una intervención on line, es perfectamente posible intervenir un proceso de comunicación que se realice en directo, o los actos que ejecute cualquier otro usuario del aparato, o que simplemente se encuentren documentos en los que aparecen terceros, o que sean titularidad de éstos, etc. En suma, como en el caso anterior, podría estarse ante situaciones en las que junto a los datos que afectan al investigado, aparezcan datos que afectan a terceros y que deben ser protegidos en el proceso.

La variada cantidad de situaciones en las que un tercero puede ver comprometido sus derechos, junto a la posibilidad de que pueda afectarse, en alguna de las diligencias de investigación electrónica, el derecho al secreto de las comunicaciones, justifica relacionar el artículo 588 bis h) LECrim, que contiene la regulación general de la afectación de terceros por la realización de cualquier diligencia de investigación electrónica, con las disposiciones que se encuentran en los arts. 588 ter b LECrim y 588 ter c LECrim, que son preceptos concretos en los que se regula la participación y/o afectación de terceros en la práctica de diligencias que consisten en la intervención de las comunicaciones. Se trata de adoptar todas las garantías necesarias cuando se ordene una de las dos diligencias de registro de datos, para que en lo posible se limite la afectación de los derechos implicados en las mismas, tomando incluso aquellas garantías que han sido reguladas específicamente para los casos en los que se afecta a algún proceso comunicativo. La Circular de la Fiscalía General del Estado 5/2019, sobre registro de dispositivos y de equipos informáticos admite esta posibilidad[229].

El art. 588 ter b, 2 de la LECrim permite, de forma general, intervenir el dispositivo empleado para la comunicación, con independencia de que el aparato sea usado de manera ocasional por el investigado como usuario; además, el precepto contempla la posibilidad de que la diligencia pueda afectar a la víctima, al permitir la intervención de su aparato para poder llegar hasta el responsable. En este segundo caso se trata de una acción de intervención completamente lógica aplicable a casos

[229] La pág. 54 de la Circular 5/2019, admite la posibilidad de que en las diligencias de registro de datos en las que pudieran resultar afectadas de alguna manera las comunicaciones se adopten las garantías previstas en la diligencia específica. Dice que «la posibilidad de interceptar comunicaciones telemáticas que brinda la diligencia de registro remoto de equipos informáticos, puede hacer que ésta sea la técnica elegida para llevar a cabo esta interceptación»

de emergencia [230] en los que concurra riesgo para la vida o la integridad de ésta. En estos casos, la medida debe venir expresamente motivada y amparada en los principios rectores que ya se analizaron en otro apartado de este trabajo, especialmente el principio de proporcionalidad.

El art. 588 ter, c LECrim, resulta más específico en lo que se refiere a la afectación de los derechos de terceros, recibiendo como denominación precisamente ese. El artículo permite intervenir tanto el terminal propiamente dicho, como el medio de comunicación telemática de un tercero (con esta alusión se abre la posibilidad de acudir a este precepto para tutelar derechos de terceros durante la práctica de la diligencia de intervención remota de equipos electrónicos). Esta intervención sólo cabe en alguno de los dos supuestos previstos: cuando el investigado se sirve del aparato, o cuando se tiene constancia o sospecha de que el tercero colabora con el investigado en la realización del ilícito penal investigado. Existe además un párrafo final que admite la posibilidad de intervenir un terminal que a su vez es intervenido por terceros de manera maliciosa.

Los tres supuestos contemplados por la ley guardan relación con el papel de terceras personas. El apartado primero se refiere al uso que el investigado hace de un terminal que no es suyo, aspecto que justifica su intervención. El segundo supuesto se sirve de situaciones en las que el tercero colabora con el investigado, incluyendo en este sentido aquéllas formulas de participación delictiva previstas en el Código Penal, incluyendo expresamente el mero beneficio del ilícito investigado. El tercer supuesto es el más complejo, ya que implica que el terminal a intervenir está a su vez intervenido por terceros, que son los que lo emplean para las finalidades ilícitas investigadas. La alusión que el precepto hace a que dicha intervención del terminal debe haber sido realizada de manera maliciosa, excluye intervenciones consentidas por el titular del aparato.

En todo caso, la norma anterior contempla los supuestos más usuales que podemos encontrar sobre la limitación de derechos de terceros, aunque sólo referida a los procesos de intervención de las comunicaciones. En el ámbito de las demás diligencias, la habilitación para afectar los derechos de terceros se encuentra en el art. 588 bis h LECrim. Esta norma es aplicable a la práctica de cualquiera de las diligencias de investigación de los Capítulos V, VI, VII, VIII y IX LECrim. A su vez, esta norma se completará con el contenido específico que cada diligencia pudiera tener sobre este aspecto específico. Esta aplicación está expresamente permitida por el precepto cuando se refiere a las diligencias contenidas en *«los siguientes capítulos»*, aunque afecten a terceras

[230] Esta intervención de las comunicaciones, o de la señal de conexión con los sistemas de cada compañía, puede servir como medio para localizar a la víctima. Ordenar la intervención de sus comunicaciones, o de sus datos asociados, puede servir para determinar su paradero. Incluso en la actualidad hay dispositivos que se conectan al teléfono móvil y que detallan si la persona está viva, mediante la realización de electrocardiogramas, avisando a servicios sanitarios, en casos de emergencia.

personas[231]. Por lo tanto, la conclusión que a la que se puede llegar es que puede acordarse una diligencia de investigación electrónica que limite tanto el derecho al secreto de las comunicaciones, como los derechos a la intimidad, la imagen, o algún otro derecho del art. 18 CE, incluso aunque con ellas se afecte a terceras personas[232]. En suma, la regla general consistirá en ver si hay una regla específica sobre la limitación de derechos de terceros para la diligencia que se quiere acordar, y cuando no exista una regla específica para la diligencia que se pretenda aplicar, se ha de acudir a la regla general, que es la de la admisibilidad de la limitación en el derecho de terceros, contenida como fórmula generalizada en el art. 588 bis h LECrim.

Alguna parte de la doctrina apunta una visión diferente sobre el papel del tercero en el ámbito de las diligencias de investigación, tomándole o considerándole como un criterio delimitador del elemento objetivo de la diligencia. El hecho de que en la investigación aparezca un tercero permite que el objeto que éste emplea (por ejemplo un teléfono o un ordenador) pueda ser el instrumento sobre el que se lleva a cabo la diligencia de intervención [233]. Por tanto, para esta interpretación se usan los bienes del tercero como medio o instrumento para dar con el responsable. Esta opinión amplía la visión del papel del tercero, y propicia intervenciones que no tienen porqué ser activas, sino que admiten la posibilidad de llegar hasta el investigado a través del tercero. La base legal de esta visión se fundamenta en el contenido del art. 588 ter b.2 LECrim, que dice que el objeto de una diligencia de intervención telefónica, o telemática, es el terminal o el dispositivo desde el que se produce la comunicación y de la que el investigado es o titular o usuario. No obstante, y ante la posibilidad de que el investigado no emplee su propio terminal, sino que utilice uno que sea propiedad de un tercero, se admite en el párrafo 1, que la intervención será posible aunque los terminales sean

[231] La doctrina considera que la fórmula elegida por el legislador a la hora de sistematizar las disposiciones comunes mueve a error, porque genera la sensación de que sólo son aplicables a una serie concreta de dichas diligencias, en concreto a las que le siguen ordinalmente o las que ella disponga al decir "los siguientes capítulos". Sin embargo la doctrina estima que estas disposiciones comunes son aplicables a todas las diligencias contenidas en el Título y que hubiera sido deseable una sistemática distinta. Así lo mantienen, por ejemplo, Marchena Gómez y González Cuellar-Serrano. Op. cit. Pág. 173-174.

[232] En todo caso hay que prestar atención al rol que el tercero tenga en los hechos investigados. No es lo mismo ser un amigo del investigado que habla por teléfono con él, o ser la víctima del tipo penal, que ser el letrado que asiste al investigado, etc, pues cada tipo de tercero puede comportar que las garantías que se deban adoptar sean diferentes.

[233] Cfr. SANCHIS CRESPO, Carolina. «Puesta al día de la instrucción penal: la interceptación de las comunicaciones telefónicas y telemáticas». *La Ley Penal* nº 125. Marzo-abril 2017. LA LEY 3914/2017. Pág. 4. En su estudio la autora realiza una exposición de las recientes modificaciones legales, sin embargo, utiliza el contenido del art. 588 bis h), en el sentido de ofrecer un punto de vista diferente a su tenor, estableciendo que su contenido puede servir para delimitar el terminal que puede ser objeto de intervención. Es decir, que lo que permite únicamente es deslindar qué aparato es el que puede ser intervenido. Dice textualmente sobre la capacidad delimitadora en cuanto al objeto que *«Los terminales o medios de comunicación objeto de intervención serán aquellos habitual u ocasionalmente utilizados por el investigado como emisor o receptor, con independencia de que sea titular o mero usuario de los mismos. También podrán intervenirse los terminales o medios de comunicación de la víctima cuando sea previsible un grave riesgo para su vida o integridad. En el caso de que los terminales o medios de comunicación pertenezcan a una tercera persona, la injerencia en la comunicación estará sometida al cumplimiento de una de estas tres condiciones: 1.ª:- Que exista constancia de que el sujeto investigado se sirve de aquélla para transmitir o recibir información. 2.ª.- Que el titular colabore con la persona investigada en sus fines ilícitos o se beneficie de su actividad. 3.ª.- Que el dispositivo objeto de investigación sea utilizado maliciosamente por terceros por vía telemática, sin conocimiento de su titular ».*

«ocasionalmente (sean) utilizados por el investigado», o de los que sea simplemente un *«usuario»*. La conclusión que ha de reafirmarse es que es posible la limitación de los derechos del art. 18 CE, incluso aunque sean de terceros, en la práctica de diligencias de investigación electrónica. Además, con la actual legislación, se admite la posibilidad de intervenir terminales que pertenecen a terceros en situaciones bastante difusas desde el punto de vista de la titularidad de dicho terminal. Es evidente que se puede intervenir en los casos en que el aparato es propiedad del tercero, pero la LECrim admite situaciones meramente posesorias, de mero uso consentido, o bien en situaciones de utilización esporádica. Estas variables deben ser argumentadas por los agentes investigadores de manera que, posteriormente, el Juez Instructor, pueda determinar el grado de frecuencia de uso del terminal por parte del tercero, a los efectos de admitir la práctica de la diligencia.

Estas normas, por el lugar concreto de la LECrim en la que se insertan, son de aplicación a las limitaciones y restricciones en el derecho al secreto de las comunicaciones, pero no hay razón que impida la aplicación de estas medidas concretas a las demás diligencias del Titulo VIII, pues lo permite la generalidad de la previsión contenida en el art. 588 bis h LECrim en lo concerniente a la afectación de terceros.

Además, las garantías que ofrecen la regulación de cada una de las concretas diligencias de investigación lo que hacen es abundar en la seguridad jurídica del tercero, por lo que es viable esa aplicación complementaria a las demás diligencias de investigación, incluso aunque afecten a otro de los derechos del art. 18 CE. En todo caso la necesidad de motivación y ponderación exigibles para su adopción vuelven a ser indispensables en este aspecto[234], pues precisamente esa labor de motivación será la que justifique la necesidad de aplicar estas normas a otros derechos que pudieran verse afectados.

En otro orden de cosas, una vez que se han visto las reglas generales sobre el modo de proceder ante los casos en que se pueden afectar los derechos constitucionales de terceros, resulta necesario concretar ante los distintos roles que un tercero puede presentar dentro de la investigación qué norma es la que corresponde aplicar, bien sea para subsumirlo propiamente en la categoría de tercero[235], bien sea para incardinarlo en otra distinta:

1.- El tercero puede guardar relación con la comisión del hecho susceptible de reproche penal, bien porque haya podido participar en su comisión como coautor con el investigado, o bien coadyuve a

[234] Vid. MARCHENA GÓMEZ, GONZÁLEZ CUELLAR- SERRANO. Op. cit. Pág. 173-174.
[235] No se debe perder de vista que pueden ser terceros una amplia gama de sujetos: personas físicas, personas jurídicas, así como también la propia víctima o inclusive el abogado del investigado, etc.

su realización a través de cualquiera de las formas de participación contenidas en los arts. 28 y 29 del Código Penal.

En este caso, dada su implicación penal en los hechos, sería perfectamente aplicable la regulación más arriba expuesta sobre las doctrinas del hecho nuevo como la del hallazgo casual, lo que conllevará la ampliación de la causa ya existente o bien el inicio de la instrucción de una nueva. En todo caso, y antes de llegar a una conclusión definitiva sobre su papel en los hechos, son aplicables las disposiciones del art. 588 bis h) LECrim, que permite la limitación general de derechos de terceros prevista para cualquier diligencia, así como también el contenido del art. 588 ter, c), apartado 2º LECrim, que faculta la intervención de un proceso de comunicación concreto de personas que participan en el hecho delictivo.

2.- El segundo supuesto es contrario al anterior, y en él es un tercero quien no guarda relación directa con la comisión efectiva del hecho, pero que sí la tiene con el investigado. Esta relación puede ser muy diversa: porque simplemente lo conozca; porque durante el proceso de intervención de las comunicaciones se ha obtenido alguna información, porque se haya empleado el terminal de esta tercera persona sin que esta conozca la trascendencia de la comunicación efectuada usando su dispositivo, etc.

En el caso de la diligencia que limita el derecho al secreto de las comunicaciones, lo determinante es que el investigado pudiera haber empleado el terminal de estos terceros. Es indiferente que los terceros sean los titulares, detentadores o usuarios del aparato, pues como dice la doctrina, «*no es determinante el aspecto dominical estricto*»[236]. Esta previsión legal tiene una finalidad ampliatoria dirigida a permitir el acceso a los terminales de otros sujetos. Por ejemplo, el uso indiscriminado de distintos terminales por varias personas, lo que suele pasar en muchas empresas, grupos, familias, etc. Nuevamente se ha de hacer una llamada de atención a esta circunstancia. El hecho de que se pueda hacer un uso esporádico por parte del investigado de un terminal electrónico, y que por eso pueda ser susceptible de intervención, requiere un esfuerzo argumentativo por parte de los agentes investigadores, en el que se justifique la necesidad de la diligencia que afecta a terceros, aún a pesar de tan escasa utilización. Como contrapartida, dicha argumentación ha de pasar el filtro de los

[236] Cfr. CAVERO FORRADELLAS, Gerardo. "*La nueva regulación de las intervenciones telefónicas en la Ley de enjuiciamiento criminal*". Ponencias de formación de fecha 27 de abril de 2016, Jornadas denominadas "La interceptación de las comunicaciones telefónicas y telemáticas": Pagina 27. https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20Cavero%20Forradellas,%20Gerardo.pdf?idFile=38380825-2079-4304-af21-40d9010e0ae9

principios rectores, en especial el de proporcionalidad de la medida, lo que requerirá un esfuerzo por parte del Juez Instructor para determinar si debe ejecutarse la diligencia, afectando los derechos de terceros, pese al uso esporádico del mismo por parte del investigado. Para ello los aspectos fácticos del supuesto son determinantes, pues dependerá de la entidad del delito, de la importancia del momento en que se encuentre la investigación, de otros posibles modos de comunicación que pueda emplear este investigado y situaciones similares.

En el caso de las diligencias de registro de datos, es posible que en la práctica de la medida se encuentre información de terceros, e incluso que el dispositivo encontrado lo sea. En este supuesto la limitación de los derechos de los terceros se hace más intensa en lo que se refiere al acceso de esta información a las actuaciones. El criterio que ha de validar el acceso será la relevancia de esa información con respecto al hecho investigado, quedando en manos del instructor expulsar de las actuaciones aquella que no se ajuste a ese interés. En lo que pudiera referirse al dispositivo, no hay inconveniente en lo que se refiere a su incautación material, y en lo que pudiera referirse al acceso a su contenido, cabe optar bien por recabar el consentimiento de su titular, bien pasar por el dictado de un auto que lo autorice.

En todos los casos en los que hablamos de la presencia de un tercero, éste puede serlo cualquiera: tanto las personas físicas como jurídicas, siendo lo indispensable que la información que esté en el dispositivo registrado le afecte. El tercero puede tener conciencia sobre los hechos delictivos o no, o tenerla o no sobre el uso del dispositivo realizado por el investigado, incluso telemático, pero en todo caso deben quedar salvaguardados sus derechos mediante la adopción de una decisión motivada que incluya una valoración de las exigencias necesarias, en particular de la proporcionalidad de la medida frente a ese tercero, que justifique acceder al contenido o datos del dispositivo.

La categoría de tercero también se extiende a aquel que guarde relación con los hechos, no con el objeto, justificándose la limitación en sus derechos, en este caso en el art. 588 bis h LECrim[237], sin perjuicio de que, si su relación alcanza al conocimiento o participación en los hechos ilícitos, pueda derivarse una corresponsabilidad penal, o sea una persona a la que pudiera aplicarse una de las excusas absolutorias del Código Penal[238].

La posibilidad de que existan terceros en el hecho a investigar será un aspecto que deberá ser informado por los investigadores en el momento de solicitar la practica de la diligencia. Haciéndolo contribuyen a advertir al Instructor de la posible limitación de los derechos de terceros, y con ello

[237] Vid. CAVERO FORRADELLAS, Gerardo. Op. Cit. Pág. 26.
[238] Véase a título de ejemplo el contenido del art. 269 del CP que exime de responsabilidad criminal al sujeto que comete delitos contra el patrimonio dentro de un determinado círculo de familiares.

cumplen con la exigencia de los arts. 588 bis. b LECrim, en relación con el art. 588 bis h, o bien 588 ter c, apartados 1º, y 2º -en su caso- de la LECrim. El oficio policial debe justificar este aspecto en lo posible, ya que el Instructor debe motivar las razones para extender la medida limitadora de derechos con respecto a esos terceros.

El papel que pueden jugar las personas jurídicas dentro del ámbito penal ha variado notablemente en los últimos años, pasando de ser entes sin responsabilidad penal, a verdaderos sujetos obligados por dichas normas. Esto las convierte en sujetos susceptibles de ser tenidos como investigados a efectos penales. En este sentido, cabe interrogarnos acerca de qué derechos fundamentales de los contenidos en el art. 18 CE son los que ostentas estas entidades, cuestión que no queda nada clara en la doctrina, que se debate entre considerarlas sujetos de estos derechos, o bien exige una regulación específica [239]. En todo caso y con independencia de los derechos que puedan asistir a la persona jurídica, como investigada, a los efectos de ser considerada como un tercero, cabe admitir que una persona jurídica sea la titular de un terminal telefónico o de un ordenador, y que estos artefactos pueden ser los empleados por el investigado para realizar la actividad antijurídica investigada. Este extremo posibilita que se lleguen a conocer por los investigadores datos e información de la persona jurídica durante la ejecución de una diligencia de investigación. En este caso, hay que distinguir entre los derechos fundamentales del investigado, que deben protegerse mediante el dictado de un auto que justifique y motive la realización de la medida o diligencia que se estime oportuna, y la protección de los intereses, que como tercero, pueda tener la persona jurídica. En este segundo aspecto, es decir, en cuanto a la protección de los intereses que como tercero, pueda tener una persona jurídica, encontramos la posibilidad de intervenir en estos intereses, en el fundamento legal contenido en el art. 588 bis h LECrim, completada, si ello fuera el caso, con el contenido concreto de la diligencia a realizar.

Esta participación, como tercero, se analiza con independencia del papel que una persona jurídica puede tener en un delito penal. En este segundo aspecto, su actividad debe ser examinada bajo el prisma de cuál ha sido su propia actuación dentro de los hechos investigados, para determinar si esta obró o no con la diligencia necesaria para evitar el delito, y por consiguiente ser tenida como investigada[240].

---

[239] En lo que afecta al contenido de los derechos fundamentales del art. 18 CE, que son los que se protegen mediante la regulación de las distintas diligencias de investigación que estudiamos, la doctrina les reconoce el derecho al secreto a las comunicaciones, y el derecho al honor. En cambio les niega el derecho a la intimidad. Vid. NEIRA PENA, Ana María. «La interceptación de las comunicaciones de la persona jurídica investigada«. *Justicia: revista de derecho procesal*. Núm 2. Año 2016. Págs. 421 a 460. En todo caso se trata de una cuestión polémica y que no queda resuelta en la ley.

[240] La STS 154/2016 de 29 de febrero de 2016. Ponente: Don José Manuel Maza Martín, realiza un profuso e interesante estudio de la nueva responsabilidad de las personas jurídicas, la cual se ha ido desarrollando desde el plano legislativo

Por último, el papel de terceros también puede predicarse de los abogados de las partes, y la intervención de sus comunicaciones debe entenderse como una medida que puede atentar contra el derecho de defensa[241], así como atentar contra el obligado secreto profesional, que constituye una causa de abstención del deber de declarar ante los Tribunales de Justicia conforme al art. 118 LEcrim. Por lo tanto, su adopción en estos casos se torna una medida a llevar a cabo sólo y únicamente en los casos previstos por las normas legales y con las demás prevenciones que más adelante veremos.

4.1. Notificación de la intervención de comunicación al tercero afectado.

La regulación actual acerca de la protección de los derechos de terceros dentro de una investigación penal, no estaría completa, y su contenido no estaría verdaderamente orientado a la tutela de los derechos contenidos en el art. 18 CE, si no existiera una protección reforzada, real y efectiva del contenido de estos derechos. La protección de los derechos mencionados no puede quedar sólo en los lapsos temporales que transcurren antes y durante la intervención de las comunicaciones, o durante la intervención de datos, sino que debe extenderse al periodo temporal posterior a la instrucción y al enjuiciamiento de la causa.

Es una novedad en nuestro derecho procesal la regulación acerca de la conservación posterior a las actuaciones instructoras y de enjuiciamiento de algunos datos concretos.

---

de forma importante en España en los últimos años. Cabe destacar que en la sentencia se analizan varias intervenciones telefónicas que determinaron finalmente que una persona jurídica se aprovechaba de la comisión de actos ilícitos. Recordemos que las personas jurídicas, tras la reforma operada en el Código Penal pueden ser eximidas del delito cometido en su favor siempre que acrediten que adoptaron las medidas necesarias tendentes a su evitación. Es lo que actualmente se denomina actuaciones de "compliance penal". Descansa en el tenor del art. 31 bis CP a cuyo tenor: «*la persona jurídica quedará exenta de responsabilidad si se cumplen las siguientes condiciones:1.ª el órgano de administración ha adoptado y ejecutado con eficacia, antes de la comisión del delito, modelos de organización y gestión que incluyen las medidas de vigilancia y control idóneas para prevenir delitos de la misma naturaleza o para reducir de forma significativa el riesgo de su comisión; 2.ª la supervisión del funcionamiento y del cumplimiento del modelo de prevención implantado ha sido confiada a un órgano de la persona jurídica con poderes autónomos de iniciativa y de control o que tenga encomendada legalmente la función de supervisar la eficacia de los controles internos de la persona jurídica; 3.ª los autores individuales han cometido el delito eludiendo fraudulentamente los modelos de organización y de prevención y 4.ª no se ha producido una omisión o un ejercicio insuficiente de sus funciones de supervisión, vigilancia y control por parte del órgano al que se refiere la condición 2.ª*».

[241] STS 79/2012, de 9 de febrero. Ponente: Don Andrés Martínez Arrieta. Se trata de la sentencia que supuso la inhabilitación de del Magistrado Baltasar Garzón. En ella se realiza un estudio acerca de las intervenciones de las comunicaciones de los investigados con sus letrados.

En segundo lugar, también es inédito, pero respetuoso con el contenido de los derechos en juego, la puesta en conocimiento de las personas afectadas, el que hayan visto limitado su derecho al secreto de las comunicaciones[242].

Nuestras normas procesales penales asumen, en lo que se refieren a estos concretos aspectos de las comunicaciones, pronunciamientos que ya habían sido tratados y adelantados por parte de la jurisprudencia del TEDH[243].

Por el contrario, en las *«disposiciones comunes a la interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos»* del Capítulo IV de la LECrim, no se aprecia deber alguno de notificar ninguna de esas diligencias mencionadas, a cualquiera de los terceros afectados por ellas.

En el Capítulo sólo se relaciona con esa obligación de conservación o no de lo obtenido, «*la destrucción de los registros»*, que da nombre al art. 588 bis k. LECrim. Es un artículo que no impone la obligación de notificar ninguna limitación practicada a los terceros. En este sentido, resulta llamativo que en sede de las normas generales para todas las diligencias de investigación electrónica no se regule nada concreto sobre la obligación de notificar la intervención realizada a terceros. Y que tampoco regule el control del contenido de las grabaciones, o de los datos que pudieran haberse obtenido, pero, en cambio, sí que se regule sobre su posible destrucción y/o conservación.

---

[242] Dice la exposición de motivos de la Ley Orgánica 13/2015, sobre el particular que «*Se pretende con ello evitar toda difusión de un material que, por su propio contenido, podría dañar de forma irreparable la intimidad del afectado»*.

[243] Vid. RODRÍGUEZ LAINZ, José Luis. *El secreto de las comunicaciones y su interceptación legal. Adaptado…* Op. Cit. Pág. 206. El autor analiza el origen y la evolución de esta obligación de notificación de las comunicaciones intervenidas en las que intervienen terceros. Cita expresamente el contenido de las sentencias del TEDH 16 de febrero de 2000 (caso Amann vs. Suiza; asunto 27978; así como las posteriores de 29 de marzo de 2005 (asunto 57752/2000), la de 21 de enero de 2010 (asunto 43757/05) y la de 3 de febrero de 2015 (asunto 30181/05), las cuales establecieron el derecho del afectado por estas intervenciones a poder tener alguna clase de reacción frente a esta injerencia de los poderes del Estado. El autor en su obra desgrana el contenido de dicha jurisprudencia que inicialmente exige tal notificación al interesado, aludiendo más tarde al contenido de otras sentencias emanadas del mismo Tribunal (páginas 218 y 219) tendentes a que tal obligación no quede sólo en el deber de notificación, sin mayor alcance, sino que sirve ello para que el afectado pueda ejercitar las acciones legales que estime oportunas, cuestionándose por este Tribunal si un tercero puede solicitar la destrucción de las grabaciones realizadas, citando sobre este particular la STEDH de 3 de febrero de 2015 (caso Pruteanu vs. Rumanía, asunto 30181/05). La legislación procesal española no regula la obligación de comunicar a terceros que se ha realizado alguna diligencia de investigación en la que aparecen, de manera general, si bien el art. 588 ter i), apartado 3 LECrim , admite en sede de la diligencia de intervención de las comunicaciones, la obligación de comunicar al tercero que se ha efectuado una grabación en la que aparece, si bien se trata de una obligación al Juez a la que se admiten importantes excepciones. También se pone de manifiesto (página 217) que el TEDH ha defendido un sistema de suspensión de la obligación de notificar a terceros las grabaciones efectuadas o las comunicaciones intervenidas, sometida a plazos.

La notificación a terceros de las operaciones de investigación realizada sobre ellos, es algo que la jurisprudencia del TEDH ha venido contemplando y exigiendo[244]. Pero, en cambio, no se ha previsto la obligación de notificar a terceros cualquier intervención en la que aparezcan, sólo se restringe esta posibilidad a los casos en que se intervienen las comunicaciones telefónicas o telemáticas[245]. Pese a ello, la Ley no impide que se aplique el contenido de las disposiciones que obligan a notificar tales acciones de investigación fuera de los casos de intervención de comunicaciones. En especial encuentro razones para hacerlo en el caso de la diligencia de registro remoto de equipos, por su especial cercanía a la intervención de comunicaciones, incluso aunque fueran comunicaciones conclusas. Y ello, aunque en tal caso el derecho afectado sea la intimidad, de manera que el acto de notificar la intervención, resulta respetuoso con el contenido del derecho del art. 18.1 y con el espíritu de la Ley.

El concreto deber de notificar la intervención practicada, en sede de intervención de comunicaciones telefónicas y telemáticas, está previsto en el art. 588 ter i, apartado 3 LECrim. Este articulo ordena realizar esta notificación, después de haberse practicado por el Juez instructor una labor de criba de información que bien sea relevante para la causa, o, al contrario, innecesaria para la misma. El precepto ordena al instructor que comunique a las personas afectadas la existencia de las intervenciones y grabaciones en las que aparecen[246]. Además, requiere que se le indiquen las concretas comunicaciones intervenidas. En todo caso, como salvaguarda, no será necesario notificar

[244] STEDH 6 de septiembre de 1978, caso Klass contra Alemania, asimismo, en la nota anterior se citan sentencias dictadas por el mismo organismo.

[245] En este aspecto de las notificaciones a terceros cabe realizar un contraste entre la STS 487/2007, de 29 de mayo. Ponente: Manuel Marchena Gómez y la STS 64/2011, de 8 de febrero, Ponente: Don Francisco Monterde Ferrer. En la primera de las citadas resoluciones en TS se encontraba en una posición tendente a rechazar la necesidad de notificar a terceros la práctica de las diligencias de intervención de comunicaciones. Así decía que «*Por otra parte, ninguna consecuencia, en orden a la integridad del derecho al secreto de las comunicaciones o al derecho a la tutela judicial efectiva, puede derivarse de la circunstancia de que la intervención judicial no fuera formalmente notificada a algunos de los que fueron destinatarios de esa medida y que, sin embargo, no habían sido imputados en las presentes diligencias. Conviene recordar que la notificación de cualquier acto procesal sólo tiene justificación respecto de las partes del procedimiento. Esa notificación adquiere una dimensión constitucional muy singular cuando se trata del imputado, en la medida en que sólo su acceso al proceso (art. 118 LECrim) le permite hacer valer el principio de contradicción, instrumento irrenunciable para la vigencia del derecho de defensa. Sin embargo, al margen del carácter secreto de las actuaciones, carecería de sentido postular el deber institucional de notificación a todos aquellos que, sin relación alguna con el objeto del proceso, pudieran convertirse en ocasionales interlocutores del imputado cuyas comunicaciones han sido intervenidas»*. En cambio, en la STS 64/2011, de 8 de febrero, el criterio se flexibiliza y cambia, pasando a la posición contraria, condicionada, eso sí, a la situación de la causa. En este punto dice esta última resolución que «*constatada la legitimidad de este recurrente en su alegación, y el hecho -como ya vimos-de que el cese de cualquier intervención telefónica debe ser notificado al interesado, cuando el estado de la causa lo permita -especialmente una vez levantado el secreto de las actuaciones- de modo que no se comprometa el curso de la investigación, el examen de las actuaciones revela que no se puede extraer la conclusión pretendida por el recurrente, y que, en consecuencia no resulta afectado el mismo por el hecho que señala»*.

[246] La medida resultará un tanto innecesaria en el caso del investigado principal, que tras ser informado de esta condición, contará con la personación de la defensa, que se encargará de las acciones procesales de impugnación a que haya lugar en su caso.

en tres situaciones muy genéricas, cuando «*sea imposible, exija un esfuerzo desproporcionado o puedan perjudicar futuras investigaciones*»[247].

El artículo se refiere al momento temporal en los que puede notificarse la existencia y el contenido de las grabaciones realizadas. El apartado primero del art. 583 ter i LECrim, establece que la fase adecuada para notificar a terceros estas grabaciones concurre cuando se alza el secreto de las actuaciones. En ese momento es público el contenido del procedimiento, tanto para las partes que se hayan personado, como para las defensas, y es necesario entregarles el contenido de las grabaciones efectuadas, para que puedan articular debidamente su derecho de defensa, y contradicción, junto al resto de la causa.

La posible afectación o limitación del derecho de terceros actúa como un filtro que permite al Instructor entregar una copia íntegra de las grabaciones, o bien dando una copia parcial de las grabaciones limitadas sólo a las que contengan hechos vinculados a las actuaciones. Esta posibilidad se da si el Tribunal indica que la razón para hacerlo es que algunas de las conversaciones afectan a terceros. Para ello, es preceptivo comunicar, de forma expresa, la ausencia de integridad de las grabaciones a los afectados, categoría que comprende según el art. 583 ter i, 1 LECrim, tanto a los investigados como a las demás partes personadas en las actuaciones[248].

Para entregar las grabaciones de conversaciones a las partes, se debe discriminar el contenido de éstas, y concretar qué personas deben quedar ajenas a la causa. De esto nacen dos obligaciones distintas: la ya citada consistente en entregar a las partes personadas el contenido parcial de las grabaciones, y en segundo lugar, notificar, a éstas últimas, que aparecen en diversas grabaciones practicadas en ella. Para que esto se haga efectivo, el Juez tiene que examinar el contenido de las grabaciones para decidir lo que queda incluido y lo que será excluido.

En caso de que las partes muestren desacuerdo, es el apartado 2 del artículo el que regula un incidente de oposición contra la decisión judicial de entrega parcial de las grabaciones. Se ha de dar

[247] Aunque a lo largo del apartado se volverá sobre ello, hay que reseñar la extraordinaria vaguedad de la obligación legal de notificar, apreciada bajo el prisma de las excepciones que se contienen en la ley para justificar la inobservancia de dicha obligación. La interpretación a las que se prestan las excepciones legales, admiten casi cualquier excusa que permita no llevar a cabo dichas notificaciones. En especial parece llamativo por lo extraprocesal, la relativa al extraodinario esfuerzo que ello pudiera comportar. Es evidente, que en la actualidad, la saturación que viven Juzgados y Tribunales, ocasiona que casi cualquier actividad suponga un esfuerzo extraordinario, razón que haría que aspectos como la falta de personal, medios de grabación adecuados, etc, justificasen un aspecto tan relacionado con los derechos constitucionales de los investigados, que es el verdadero foco de atención en el que hay que centrar la reforma procesal.

[248] Vid. RODRÍGUEZ LAINZ, José Luis. *El secreto de las comunicaciones y su interceptación…* .Op. Cit. Pág. 214. Además el autor distingue entre las labores propias del Juez Instructor como responsable último de la decisión de entrega de las grabaciones efectuadas, y las funciones propias del LAJ - Letrado de la Administración de Justicia- como responsable del contenido de las actuaciones y de la efectiva labor de entrega. No obstante el autor defiende que el encargado de examinar el contenido de las grabaciones a los efectos de poder determinar qué parte de las mismas deben quedar excluidas al Juez, contrastando con la obligación que hasta la reforma tenía el Secretario Judicial de efectuar la escucha, el cotejo así como de supervisar la transcripción o incluso posible traducción.

un plazo a las partes (que no está fijado legalmente, pero que sí debe verse condicionado en función al volumen de información a examinar) para que manifiesten si estiman necesario o no la aportación de las grabaciones que fueron excluidas por el Instructor, garantizándose así la contradicción[249].

Lo siguiente que se establece es la obligación del Juez Instructor para que, de forma activa, oiga las grabaciones (pues dice el tenor literal del precepto que el mismo «*oídas y examinadas por sí esas comunicaciones»*), para que tras ello decida si entrega todas las grabaciones o se mantiene en la decisión de entregar su contenido parcial. Resulta llamativo que el texto legal no indique si dicha resolución es recurrible, lo que debe interpretarse en sentido afirmativo, porque es una decisión judicial sometida a control.

El párrafo tercero contempla la obligación de notificar a las terceras personas que, no siendo investigadas, aparecen en las grabaciones. La comunicación que se realice a estas terceras personas abarca el hecho mismo de la grabación, y en segundo lugar la de comunicar las concretas conversaciones en la que haya participado.

La doctrina entiende que el concepto de tercero ha de entenderse de manera amplia, extendiéndose a cualquiera que aparezca en las actuaciones como participante de alguna de las conversaciones, sin que las excepciones legales excluyan el derecho a ser notificados[250].

El artículo fija varias excepciones a esta obligación de notificar. Son excepciones muy generales cuyo uso permite limitar o eliminar la práctica de estas notificaciones, que por otro lado figuran como obligatorias. Las excepciones se resumen en tres categorías:

- que sea imposible efectuar la notificación.
- que el hecho de practicarla exija un esfuerzo desproporcionado.
- que haciéndolo puedan perjudicarse futuras investigaciones.

La doctrina ha criticado bastante el alcance de las excepciones[251] contenidas en la Ley, porque su alto grado de generalidad posibilita dejar sin contenido este derecho tan importante. Notificar la

[249] No debe perderse de vista que han de conjugarse por una parte, el derecho del tercero a conocer con qué grabaciones se cuenta por parte del Juzgado Instrcutor, pero también ha de protegerse el derecho de los distintos terceros entre sí, de manera que unos y otros no deben conocer los datos de terceros, así como los del propio investigado. Por lo tanto pese a lo acertado de la medida, lo más adecuado parece ser efectuar dichas entregas parciales, y continuar con la postura denegatoria de la entrega completa, precisamente en aras a proteger los datos de los demás terceros afectados por las grabaciones realizadas.

[250] Cfr. RODRÍGUEZ LAINZ, José Luís. *El secreto de las comunicaciones y su interceptación*…..Op. cit. Pág. 211. El autor es consciente de que existen limitaciones en la notificación a terceros. Dichas limitaciones se deben ser en mayor medida aplicables a quien teniendo participación en el proceso ya ven respetado estos derechos de alguna otra manera, pero no defiende que otros terceros se vean tan afectados en este conjunto de exclusiones, porque esto sería *«convertir en regla general esos conceptos de imposibilidad o gravosidad de cumplimiento de la obligación de comunicación»*

[251] Vid. RODRÍGUEZ LAINZ, José Luis. *El secreto de las comunicaciones y su interceptación* Op. cit. Pág. 210.

existencia de la grabación es lo más respetuoso con el derecho fundamental al secreto de las comunicaciones, y acudir a vías tan generales para excepcionar esta obligación, deja esta garantía sin contenido, o bien muy disminuido.

Las circunstancias exonerantes del deber de notificación a terceros son fácilmente aplicables casi a cualquier situación, lo que permite prever que será lo más habitual, ampararse en ellas para evitar cumplir con esta obligación. Y es que, situaciones que desborden la instrucción, puedan influenciarla o incluso hacerla carecer de objeto pueden ser muchas. La doctrina invoca una interpretación flexible de estos supuestos, considerando que no debe procederse a notificar la existencia de grabaciones, por ejemplo cuando se ignore la identidad del interlocutor que ocupa la posición de tercero, y cuando no quede justificada una labor de investigación tendente a determinarla, o aquéllos casos en que de hacerse tal notificación pudiera afectarse el derecho a la intimidad de las personas, o a su buen nombre[252].

El legislador parece haber insertado estas excepciones, con el fin de liberar de la carga al Juez de hacer efectivas tantas notificaciones, pero no a cualquier precio, sino bajo una justa causa. La utilidad de estas excepciones parece clara, sobre todo en aquellas instrucciones penales en que se han practicado muchas intervenciones, y consecuentemente haya muchos teléfonos afectados, con muchos terceros relacionados, etc. En estos supuestos efectuar las notificaciones se antoja como un acto muy complejo y laborioso, y el consumo de recursos humanos y materiales parece injustificado. Y no debe perderse de vista, que es posible evitar la notificación cuando llevándose a cabo, haría peligrar alguna otra investigación[253].

El afectado, además del derecho a ser notificado, cuenta con la facultad de obtener una copia de las grabaciones efectuadas, si lo pide. La excepción, tanto a la notificación como a la entrega de la copia, reside en que cuando haciéndolo, se ponga en peligro el derecho a la intimidad de otras personas, o resulte contrario a los fines del proceso, será posible no llevarlo a la práctica. La consecuencia de la falta de entrega de las grabaciones tras haber notificado su existencia no está prevista. Tampoco lo está la consecuencia derivada de la ausencia de la notificación de la

[252] Vid. RODRÍGUEZ LAINZ, José Luís. *El secreto de las comunicaciones y su interceptación…*Op. cit. Pág. 211. El autor piensa en este caso, por ejemplo, en personas que, perteneciendo a la alta sociedad, podrían ver afectado su buen nombre al conocerse que compran sustancias estupefacientes para su propio consumo.

[253] Personalmente estimo que establecida la obligación de comunicar las concretas comunicaciones intervenidas, no debe ser excusa para notificar al afectado el hecho de que fuera complejo determinar qué comunicaciones fueron intervenidas en el caso de que hacerlo exija " *un esfuerzo desproporcionado*", pues los oficios policiales van relatando las comunicaciones practicadas con su fecha de realización y los tiempos de duración de las mismas, con lo que se trata sólo de localizarlas en las actuaciones o simplemente solicitar de las autoridades policiales un listado de las practicadas. Por el contrario resulta lógico no llevarlo a cabo cuando es imposible, o cuando haciéndolo peligran otras investigaciones. En este sentido, Vid. RODRÍGUEZ LAINZ, José Luis. *El secreto de las comunicaciones y su interceptación…*Op. cit. Pág. 215, que pone el ejemplo de una célula de grupo terrorista de la que siendo investigada aún no se han encontrado datos concluyentes sobre su actuación delictiva.

grabación. La doctrina defiende una absoluta neutralidad procesal en lo que a la causa se refiere por la falta de *«la comunicación a estos terceros ..en modo alguno incide sobre la regularidad constitucional del acto de injerencia»*[254]. La consecuencia que se deduce es que la diligencia no se verá afectada de nulidad pese a que no se notifique a los terceros afectados.

En conclusión, destaca en la nueva regulación el reconocimiento del derecho de los terceros a conocer que se han efectuado grabaciones de conversaciones en las que ellos mismos, como sujetos ajenos y distintos del investigado intervienen, así como a conocer de qué tipo de comunicaciones se dispone, y de cuánta información personal dispone el Estado[255] , todo eso para reaccionar en la medida en que se estime oportuno por el afectado[256].

El interrogante que se abre es cuál pueda ser la reacción de un tercero sabedor de la existencia de grabaciones en las que aparece él como afectado. La ley no concede ni tampoco niega acciones de ninguna clase, salvo la concreta petición al Juez Instructor de las copias de las grabaciones.

La doctrina considera que la acción más probable que pueda solicitarse sea la petición al Juez Instructor para que sean destruidas las grabaciones en las que aparece el solicitante. Esta posibilidad se abre incluso aunque el tercero afectado no esté personado en las actuaciones, ni cuente con ninguna posición procesal. La doctrina considera que el derecho a ser notificado es la habilitación suficiente para solicitar esa destrucción, pues de lo contrario se habría creado un derecho, que quedaría sin contenido[257]. La opinión particular que sostengo es que no parecen existir razones que impidan la práctica de esta petición de destrucción siempre y cuando las grabaciones en las que aparece el tercero no hayan resultado de interés para la causa. Admitir la destrucción de las que sí tuvieron interés supondría poder limitar los deberes de conservación y privar de eventuales evidencias que pudieran resultar esenciales para la decisión sobre la pretensión penal ejercitada.

5. El aseguramiento de los datos.

---

[254] Cfr. RODRÍGUEZ LAINZ, José Luis. *El secreto de las comunicaciones y su interceptación…*Op. Cit. Pág. 212.
[255] Vid. MARCHENA GÓMEZ, GONZÁLEZ CUELLAR- SERRANO. Op. cit. Pág. 274.
[256] Ciertamente la norma carece de cualquier derecho derivado de tales intervenciones, salvo, claro está el derecho a poder conocer primero la existencia y luego el contenido de tales grabaciones. No estimo que fuera posible esgrimir contra el Estado reclamación alguna por un deficiente servicio público, o responsabilidad por el anormal funcionamiento de la Administración, pues precisamente durante el ejercicio de la investigación penal (acto que corresponde en exclusiva a los poderes del Estado) se ha logrado obtener esta información.
[257] Cfr. RODRÍGUEZ LAINZ, José Luis. *El secreto de las comunicaciones y su interceptación…*Op. cit. Pág. 220 y 221. Dice textualmente el autor que *« el reconocimiento del derecho a la obtención de copia no es en sí un fin, sino más bien un medio a partir del cual poder canalizar el ejercicio de acciones derivadas de la afectación de derechos fundamentales»*- El autor defiende un claro papel activo de los afectados en orden a pedir la exclusión y destrucción de cuanto les afecte.

La sensibilidad que la nueva regulación presenta con el contenido de los derechos del art. 18 CE se extiende, no sólo a los derechos de terceros afectados, sino también a cómo conservar y proteger los datos obtenidos durante la investigación. La preocupación por la obtención de los datos, como el objeto de la investigación, se hace patente en la nueva regulación procesal a través de varias medidas.

Unos medios de protección del contenido de las actuaciones, y su preservación del conocimiento por parte de terceros, son más conocidos procesalmente que otros. Por ejemplo, a lo largo de la instrucción, la figura del secreto de las actuaciones es la forma más importante de proteger el acceso a los datos, y durante el enjuiciamiento cabe acordar la vista a puerta cerrada; pero con posterioridad al juicio oral, las medidas de protección se difuminan, siendo que hay algunas diligencias de investigación (como la que consiste en la intervención de comunicaciones orales), que presentan su propia normativa específica, dirigida a conservar algunos de estos datos más allá de la conclusión de las actuaciones. En lo que afecta al contenido de este apartado, hemos de ubicarnos en el momento inicial de la investigación, concretamente al inicio de la misma, cuando aún no se cuenta con orden judicial que permita el registro de dispositivos que albergan la información que se considera necesaria para avanzar en el conocimiento de los hechos, pero en todo caso se sabe quién puede tener tal información, y se necesita preservar del conocimiento público este material, para que puedan ser los investigadores los que tengan un primer acceso al mismo.

Desde este punto de vista, la nueva regulación de la LECrim dispone medidas para que los datos se guarden y conserven hasta que se disponga de esa resolución judicial habilitante para el acceso y registro. Estas medidas están en el Capítulo X del Título VIII LECrim, último de los capítulos del Título, y también concede facultades al Ministerio Fiscal para evitar que los datos de interés para la investigación se pierdan. El Capítulo se denomina *«medidas de aseguramiento»*, título que implica y sugiere la necesidad de otorgar una protección integral de los datos tanto desde el inicio, como durante toda la instrucción de la causa.

El término aseguramiento que se emplea en el Capítulo X se dirige a evitar la pérdida o alteración de datos, pero la nueva regulación no desconoce de otras medidas dirigidas a salvaguardar, proteger y asegurar datos, aunque en estos otros casos, la protección esté pensada para momentos distintos al inicial[258].

En suma, puede apreciarse en la nueva regulación una preocupación por el aseguramiento de los datos que se extiende durante toda la investigación, desde la fase inicial de investigación policial,

[258] Por ejemplo, el art. 588 bis k LECrim, en sus tres párrafos, que además son preceptos comunes, y de aplicación general a todas las diligencias del Título VIII, contempla cómo eliminar los datos obtenidos cuando el proceso se ha terminado, y cómo asegurar una presencia de los mismos por si fuera necesario volver a usarlos.

pasando por la fase de instrucción propiamente dicha, siguiendo por la fase de juicio oral, y alcanza más allá del enjuiciamiento definitivo.

Esta búsqueda de un nivel adecuado de protección va dirigida a evitar la difusión de algún contenido indeseado, a la conservación de los datos obtenidos y a la correcta eliminación de todos los datos innecesarios. El entronque de estas finalidades con la protección de los derechos que tutela el Título VIII [259], sirve para cerrar un tratamiento procesal penal integral de los mismos.

En esta labor de aseguramiento de los datos en el inicio de las actuaciones destaca la función del Ministerio Fiscal.

El art. 588 octies de la LECrim[260] es el único precepto que contiene el Capítulo X del Titulo VIII. El precepto puede ubicarse, desde una óptica temporal, en una fase inicial de la investigación, en la que o bien la Policía Judicial o el Ministerio Fiscal, son conocedores de la posible existencia de una serie de datos que pudieran resultar de utilidad en la investigación emprendida, pero aún no cuentan con autorización para poder obtenerlos. No obstante, precisamente por el hecho de no tenerlos aún a su disposición, los investigadores son conscientes de la posibilidad de que éstos, o parte de su contenido, se malogren por el transcurso de tiempo que va desde que se interesa la diligencia para obtenerlos, hasta que el Juez resuelve sobre dicha petición, y se llega efectivamente a ejecutar la medida de intervención de los mismos.

Esta circunstancia permite entender el contenido del apartado primero, que otorga tanto al Fiscal como a las Fuerzas y Cuerpos de Seguridad, la facultad de ordenar a una persona física o jurídica

[259] La Exposición de Motivos de la Ley Orgánica 13/2015 establece que la finalidad de estas disposiciones es la de *«fijar los términos de borrado y eliminación de las grabaciones originales, una vez se ponga termino al procedimiento"*. Sigue diciendo la norma que la finalidad que se persigue con ello es la de *«evitar la difusión de un material que pudiera dañar de forma irreparable la intimidad del afectado»*.

[260] Igualmente la Exposición de Motivos de la Ley Orgánica 13/2015 manifiesta sobre el particular que la finalidad de la norma es evitar que la aportación de los datos e informaciones se «*vea frustrado por la desaparición, alteración o deterioro unos elementos inherentemente volátiles»*. Se advierte que el origen de esta norma está en el artículo 16 del Convenio sobre Ciberdelincuencia, de 23 de noviembre de 2001. Debe recordarse que el contenido de este precepto establece bajo la rúbrica de *«Conservación rápida de datos informáticos almacenados»* lo siguiente:

«21. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para permitir a sus autoridades competentes ordenar o imponer de otra manera la conservación rápida de determinados datos electrónicos, incluidos los datos sobre el tráfico, almacenados por medio de un sistema informático, en particular cuando existan razones para creer que los datos informáticos resultan especialmente susceptibles de pérdida o de modificación.

2. Cuando una Parte aplique lo dispuesto en el anterior apartado 1 por medio de una orden impartida a una persona para conservar determinados datos almacenados que se encuentren en posesión o bajo el control de dicha persona, la Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a esa persona a conservar y a proteger la integridad de dichos datos durante el tiempo necesario, hasta un máximo de noventa días, de manera que las autoridades competentes puedan conseguir su revelación. Las Partes podrán prever que tales órdenes sean renovables.

3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar al encargado de la custodia de los datos o a otra persona encargada de su conservación a mantener en secreto la aplicación de dichos procedimientos durante el plazo previsto en su derecho interno.

4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15».

que retenga y conserve esos datos, sin merma alguna de su contenido íntegro, hasta que cuenten con la autorización judicial necesaria para poder obtenerlos.

El deber de conservación que los investigadores pueden imponer al tenedor de los datos está sujeto a un plazo temporal, con lo que no es una retención indefinida ni ilimitada. En todo caso, lo destacable del contenido de la norma no es el plazo durante el que debe conservarse la información, sino que se está ante una orden de debida observancia para el requerido, con consecuencias penales si no se cumple[261].

El precepto impone al tenedor de los datos dos obligaciones muy concretas. La primera es conservar los datos bajo su poder durante noventa días. Este plazo puede ser ampliado, sólo una vez más, otros noventa días, hasta llegar a un total de ciento ochenta días. La segunda obligación impuesta al tenedor de los datos es guardar el secreto sobre los datos a conservar y sobre la petición que le ha sido realizada. Estas dos obligaciones dependen de la obediencia de la orden.

Durante el plazo de conservación de la información, el artículo no prevé cómo ha de controlarse el cumplimiento de esta obligación de retención y de conservación de los datos.

Además, el precepto tampoco dice cómo computar el plazo de retención de la información. Al respecto, puede entenderse que el plazo se computa desde que se haya realizado la petición de la diligencia de registro de datos, cuyo contenido se ha ordenado conservar, o bien también cabe entender que dicho plazo se computa desde que se notifica, de alguna manera, al obligado a conservar los datos, que cumpla dicha orden de conservación. En todo caso, no se debe perder de vista que el hecho de que el texto legal no haga mención alguna a cómo se debe computar el plazo, supone en la práctica una enorme flexibilidad en las posibilidades que, en ocasiones, puede tener trascendencia, precisamente en orden a entender que la obligación de conservación ha decaído o no.

El plazo de noventa días se muestra bastante ajustado a la finalidad que debe cumplir, más si lo comparamos con otras obligaciones que también están sometidas a plazo en el texto de la LECrim, como la que ha sido impuesta al Juez Instructor para dictar su resolución estimatoria o desestimatoria de la diligencia de registro, que es una plazo más breve y ajustado. Sin embargo, ante la posibilidad de que se demore la obtención de los datos del correspondiente registro, el legislador ha creído oportuno otorgar más margen, un segundo plazo, hasta un total de ciento ochenta días de retención y conservación de la información[262].

[261] Principalmente las consecuencias derivadas de la ausencia de colaboración son de orden penal, pues se incurriría en un delito de desobediencia, previsto en el art. 556 CP.

[262] El tenor del artículo está redactado de manera que el acento se coloca en los plazos de retención. Por el contrario nada se dice en el precepto acerca de las motivaciones que puedan llevar a necesitar de la ampliación del plazo de retención, ni tampoco de las exigencias, requisitos o presupuestos para que opere dicha ampliación, como por ejemplo,

El tenedor de la información, además del deber temporal de conservación, ha de guardar secreto sobre los datos, el contenido de éstos, y de la orden de conservación o aseguramiento. En el caso de contravención de estas exigencias, se verá sujeto a las responsabilidades que se contienen en el art. 588 ter e LECrim, párrafo tercero, que advierte de la comisión de un delito de desobediencia.

La regulación de la conservación de la información no estaría completa si sólo estuviese dirigida a intentar evitar la pérdida de los datos de los que aún no se dispone, sino que, además, se aprecia una segunda preocupación en la ley, que es la que se refiere al aseguramiento de datos, si bien en este aspecto ya no estamos ante una fase inicial de la investigación, sino que el aseguramiento se extiende durante la causa e incluso su finalización. En este segundo asunto, el del aseguramiento de la información obtenida, se trata de conjugar el derecho a la intimidad, la propia imagen y el honor de los investigados o enjuiciados, con las necesidades de archivo y recuperación de los datos de la causa cuando fuera necesario. En este sentido, el artículo 588 bis k LECrim es el que, con carácter de disposición general, completa el aseguramiento, pero en este caso, dirigido a un momento posterior al enjuiciamiento. La rúbrica es una clara manifestación de su contenido, ya que el precepto se titula de la *«Destrucción de registros»*.

El párrafo primero ordena eliminar los registros originales realizados mediante el empleo de los sistemas informáticos elegidos para limitar el derecho afectado en cada caso[263]. Cumpliendo con el precepto se deben eliminar de SITEL, VALHALA, o de cualquier otro sistema similar empleado para la escucha, registro o acceso realizado, cualquier rastro de la intervención efectuada. Además, no es la única disposición sobre el destino de los datos una vez acabada la causa.

Una vez se llega a la finalización de un proceso penal, tras la oportuna sentencia, y de la declaración de su firmeza, su contenido se archiva, quedando éste al servicio de la administración de justicia, y de las partes, por si fuera necesaria para cualquier acción, o a los meros efectos de guardar copia de lo realizado. En cuanto a los datos, y las grabaciones, se ordena que el Letrado de la Administración de Justicia guarde una copia, bajo su custodia, de estos registros, una vez firme la resolución que

---

la necesidad de acreditar que se ha solicitado judicialmente la intervención, o las razones por las que dicha diligencia aún no se ha ordenado, etc. Asimismo tampoco se ha dispuesto nada que evite la lesión de los derechos del art. 18 CE durante el plazo de retención. Hubiera sido deseable un mayor detalle a la hora de regular las condiciones para que los datos que son retenidos no se vean menoscabados de ninguna forma, así como regular las condiciones bajo las cuáles se puede pedir la ampliación de la retención, ya que la ausencia de toda disposición sobre estos aspectos admite una indeseable amplitud interpretativa en materias que se refieren a derechos fundamentales.

[263] Vid. RIOS PINTADO, Juan Francisco. "La reforma procesal. Incorporación al proceso de los datos de tráfico; preservación específica de datos informáticos (arts. 588 ter j y 588 octies de la Ley de Enjuiciamiento Criminal)". Ponencias de formación realizadas por la Fiscalía general del Estado de 10 de marzo de 2016. Página 13. Fuente:https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20Rios%20Pintado.pdf?idFile=9bb2604a-0ca5-432c-8124-f51611957c7b.

pone fin al procedimiento. El artículo no indica cómo debe ejecutarse esto[264]. Este registro del Letrado de la Administración deberá ser destruido cuando transcurran cinco años desde la firmeza de la resolución final del procedimiento.

En este aspecto la norma es muy exhaustiva, al recoger las distintas situaciones por las que el proceso puede finalizar: por prescripción (de los hechos o de la pena), por sobreseimiento, por sentencia absolutoria, etc. Sin embargo, si a juicio del tribunal se considerase que es necesario conservar los registros existentes, se mantendrán[265].

Para asegurar la conservación debe dictarse una resolución judicial expresa y motivada, con forma de auto, donde se exprese el juicio de necesidad de dicha conservación, y se ordenen la preservación más allá del plazo de cinco años inicialmente reconocido por la ley[266].

El precepto no ofrece las razones para que la conservación más allá de cinco años pueda considerarse justificada, de modo que habrá de ser el auto que la acuerde el que las explicite[267], para, que de este modo, se pueda conocer el juicio de razonamiento y motivación.

Por último, cabe señalar que los Tribunales darán las instrucciones necesarias a la policía judicial para que cumplan con todo lo ordenado en relación tanto al suministro de información que se deba conservar como aquélla que se ordene eliminar o destruir.

B. Aspectos específicos.

Una vez que han sido expuestos los presupuestos y requisitos generales exigibles para la adopción de cualquier medida limitadora de los derechos del artículo 18 CE, se seguirá con el estudio de las diligencias de investigación tecnológicas de acceso a dispositivos de almacenamiento masivo de datos y de intervención remota de equipos electrónicos.

[264] La falta de disposición legal sobre este aspecto abre la posibilidad a que la conservación de la información se realice de cualquiera de las formas posibles. A título de ejemplo, se puede conservar en los propios autos, o lo que es más probable, en alguna de las piezas separadas que obligatoriamente se debieron aperturar al momento de acordar la diligencia que permitió la obtención de la información, así como conservar los dispotivos electrónicos en que dicha información quedó archivada. En todo caso la ley admite que el Letrado de la Administración conserve estos datos del modo en que considere más oportuno.

[265] Vid. RIOS PINTADO, Juan Francisco. Op. Cit. Pág. 13. El autor defiende la necesidad de dar audiencia a las partes que pudieran verse afectadas a los efectos de poder oír a cada una de ellas antes de decidir. Aunque el autor no lo indica estimo que igualmente resulta necesaria la audiencia del Ministerio Fiscal en cuanto que garante de los derechos constitucionales de los afectados.

[266] Puesto que el precepto habla de Tribunales, excluye por lo tanto que la orden de conservación se haga por diligencia de ordenación del Letrado de la Administración de Justicia.

[267] Estimo que las razones pueden ser múltiples y no siempre relacionadas con los aspectos propios de la causa, sino también por razones históricas, de enseñanza, difusión jurídica de relevante interés, etc.

Las dos diligencias constituyen una novedad introducida por el legislador en la reforma de la Ley de Enjuiciamiento criminal del año 2015, y por eso resulta conveniente ofrecer, antes de analizar su contenido específico, un análisis de los distintos aspectos, tanto fácticos como jurídicos, que han influido en su introducción en la LECrim.

Esta visión comprenderá el estudio del debate legislativo de la norma aprobada, la legislación de otros países de nuestro entorno geográfico y cultural, la influencia de algunos instrumentos internacionales, y la influencia de la jurisprudencia sobre estos métodos de investigación basados en el registro de dispositivos electrónicos.

1. Evolución, configuración y antecedentes de la normativa actual.

1.1. Génesis, debate y desarrollo de la normativa procesal vigente.

El objetivo de la Ley Orgánica que reguló las diligencias de investigación electrónica estaba completamente justificado por las razones que ya se han ido desgranando. El carácter de ley orgánica también quedaba suficientemente evidenciado, en tanto que la materia afectaba derechos fundamentales. Finalmente, la Ley Orgánica 13/2015 denominada «*Ley de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica»* ha regulados las materias que afectan, de una u otra forma, a los derechos fundamentales, circunscritos específicamente a los contenidos en el art. 18 CE.

El hecho de que la norma fuera a afectar, limitar o influir en la interpretación de determinados derechos fundamentales, motivó un interesante debate durante la aprobación de la Ley. Dicho debate legislativo no se ciñó sólo a las diligencias de investigación electrónica, sino que también se detuvo en otras materias de importante calado procesal. Entre esas otras materias pueden citarse el derecho de defensa, la conexidad delictiva, la remisión de atestados por la Policía al Juzgado, la fijación de plazos máximos en la instrucción de las causas penales, la introducción del procedimiento monitorio penal[268], la nueva denominación de los antiguos imputados (ahora

[268] La Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y regulación de las medidas de investigación tecnológica recibió una tramitación parlamentaria paralela a la que más tarde llegó a la ser la Ley 41/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para la agilización de la Justicia Penal y el fortalecimiento de las garantías procesales. Dado que esta última norma citada contenía algunos de los aspectos señalados, muchos de los debates se centraron más en el contenido de esta última que en un más serenos y sosegado debate de la primera de las leyes

investigados), etc. También regularía la facultad de los Cuerpos y Fuerzas de Seguridad para que, en situaciones de emergencia, pudieran acordar ciertas diligencias limitativas de derechos fundamentales, dando cuenta al Juez en breve plazo, siendo esta concreta cuestión, la que en mayor medida monopolizó el debate. En todo caso estas materias fueron reguladas por dos leyes, una orgánica, y otra ordinaria, que pese a diferenciarse entre sí, contaron con un debate conjunto en el que se trataron todos los asuntos sobre los que estas normas iban a versar, con independencia de que afectase o no, a derechos fundamentales.

Este carácter conjunto de todos los debates hizo que se echase en falta un análisis más profundo, rico y particular sobre los problemas que planteaba la nueva regulación prevista. En especial, se echó de menos algún debate que en exclusiva tratase las diversas diligencias de investigación tecnológica, dado que el se produjo sobre esta concreta cuestión fue escaso, y casi que nos atreveríamos a decir, superficial.

La novedosa regulación de las diligencias de investigación electrónica contenidas en la Ley Orgánica 13/2015, de 5 de octubre era muy esperada por la doctrina[269], ya que ninguna de estas nuevas diligencias encontraba acomodo legal en nuestro derecho positivo previo. Además, no se debe olvidar que la Ley aprobada también contenía una nueva configuración de aspectos como el derecho a la asistencia letrada -art. 118 LECrim-, y de los derechos implicados en una detención -art. 520 LECrim-; así como una nueva regulación de la situación de prisión incomunicada -art. 527 LECrim-, trasponiendo sobre esa cuestión la normativa europea sobre la materia.

Esta importante diversidad de medidas que se regulaban en el Proyecto de Ley justificaban el intenso contenido de los debates legislativos que se produjeron, centrados en su mayor parte en los aspectos más polémicos de cada una de estas materias, bien fuera las que se recogieron en la ley ordinaria[270] como en la orgánica, modificadoras las dos de la LECrim[271].

---

citadas. De hecho alguno de los diputados expusieron una queja sobre este aspecto en sus intervenciones criticando el modo en que les fueron remitidas las normas para su debate y aprobación.

[269] Vid. OTAMENDI ZOZAYA, Fermín. *Las últimas reformas de la Ley de Enjuiciamiento Criminal. Una visión práctica tras un año de vigencia*. Dykinson. Madrid. 2017. Pág. 23.

[270] La Ley Orgánica 41/2015, de 5 de octubre, fue objeto de debate de forma simultánea con la ley que también afectaba a la Ley de Enjuiciamiento Criminal que fue finalmente la Ley 41/2015, de 5 de octubre para la agilización de la Justicia pena y el fortalecimiento de las garantías procesales.

[271] En el siguiente enlace web ofrecido por el Congreso de los Diputados http://www.congreso.es/portal/page/portal/Congreso/Congreso/Iniciativas?_piref73_2148295_73_1335437_1335437.next_page=/wc/servidorCGI&CMD=VERLST&BASE=IW10&FMT=INITXDSS.fmt&DOCS=1-1&DOCORDER=FIFO&QUERY=(121%2F000139*.NDOC.), puede constatarse el devenir que siguió la tramitación de la norma en el Congreso de los Diputados, y es que la norma procesal finalmente aprobada fue antes el proyecto de Ley 121/000139, y fue publicada como tal iniciativa en el BOCG Congreso de los Diputados Serie A , Núm. 139-1, de 20 de marzo de 2015. Es de destacar que la propuesta de redacción que se refiere a los arts. 588 sexies, apartados a hasta c, y los arts. 588 septies, apartados a hasta c presentan la misma redacción que más tarde constituirían la norma positiva publicada en el BOE. El trámite de enmiendas al proyecto se publicó en el 29-05-2015 en el BOCG núm. A-139- 2. El informe de la ponencia se publicó el día 10-06-2015, en el BOCG núm. A- 139- 2; el dictamen de la

El análisis de los debates legislativos que dieron origen a las dos leyes constituye una labor compleja, pero interesante e instructiva, porque analizar el contenido de los intercambios de parecer en sede parlamentaria permite conocer qué aspectos fueron los más debatidos, lo que permite colegir qué materias ocasionaban una mayor preocupación.

En este sentido, puede constatarse que el mayor, y más intenso debate parlamentario se centró fundamentalmente en las materias que no fueron propiamente la investigación electrónica [272], sino las que quedaron reguladas por la ley ordinaria.

El contenido de los debates fue más intenso en el Congreso de los Diputados, mientras que, en cambio, en el Senado hubo muy poca adición y complemento por vía de enmiendas, en especial a lo referido a las diligencias de investigación electrónica[273].

Además, también puede comprobarse como el debate de las dos diligencias de acceso y registro de datos contenidos en dispositivos electrónicos no suscitó casi controversia entre los parlamentarios, dado que no existió casi ninguna duda o un rechazo frontal por parte de los grupos respecto de las mismas. De hecho, lo poco que se debatió sobre estas diligencias concretas se refirió a simples puntualizaciones o mejoras en su configuración global, sin que se manifestara ninguna posición que fuera contraria a su inclusión y recogida en la norma procesal penal, ni tampoco se presentó por ninguno de los Grupos de la Cámara una propuesta de redacción distinta con respecto a la presentada a debate por el Ministerio de Justicia.

En consecuencia, ambas medidas de investigación electrónica pueden considerarse como medidas necesarias, útiles y convenientes, a ojos de todos los grupos que debatieron sobre ellas. La ausencia

---

Comisión junto a los escritos de mantenimiento de enmiendas para su defensa en el Pleno se publicó el día 16-06-2015, en el BOCG a-139-4. La aprobación por el pleno se publicó el día 19-06-2015 en el BOCG a-139-5.

[272] http://www.congreso.es/portal/page/portal/Congreso/PopUpCGI?CMD=VERLST&BASE=pu10&FMT=PUWTXDTS.fmt&DOCS=QUERY=%28DSCD-10-PL-278.CODI.%29# (Página 9). En el anterior enlace, en el que se puede leer el contenido del Diario de sesiones del Congreso de los Diputados, Pleno y Dip. Permanente, núm. 278 de 30-04-2015 cve: DSCP-10-PL-278, con las comparecencias efectuadas por los diversos grupos parlamentarios en el debate a la totalidad efectuado para aprobar la norma. Destacamos el contenido de las páginas 13, 22, 23, 26, 29, 31 y 32. En estas intervenciones se aprecia un consenso entre todos los grupos parlamentarios en relación a la necesidad de proceder a regular la materia relativa a la investigación tecnológica y ello porque nuestra legislación procesal penal carecía completamente de cualquier regulación más allá de las intervenciones telefónicas. No obstante, claro está, cada grupo realiza una crítica a aspectos que relacionados con la regulación propuesta: así la mayor parte se decanta por criticar las posibles intromisiones efectuadas por los Cuerpos y Fuerzas de seguridad en una situación de emergencia, y ello pese a que deban dar cuenta en un plazo muy breve al juez de instrucción; también se critica el plazo máximo de duración de las posibles escuchas; el catálogo tan amplio de delitos a los que se pueden aplicar estas medidas de intervención, etc.

[273] Es destacable reseñar que no existieron modificaciones en la tramitación de la norma en el Senado, con respecto a la iniciativa presentada en el Congreso por parte del Ministerio de Justicia. Con ello se constata que se devolvió al Congreso para su aprobación el mismo texto, que sobre estas diligencias de investigación, fue propuesto. Así puede apreciarse de la lectura de las enmiendas efectuadas en el Senado y que fueron publicadas en el BOCG, Congreso de los Diputados, Serie A, núm. 139-6, de 17 de septiembre de 2015 cve: BOCG-10-A-139-6. Se puede apreciar en el siguiente enlace ofrecido por la propia página web del Congreso: http://www.congreso.es/portal/page/portal/Congreso/PopUpCGI?CMD=VERLST&BASE=pu10&FMT=PUWTXDTS.fmt&DOCS=1-1&DOCORDER=LIFO&QUERY=%28BOCG-10-A-139-6.CODI.%29#(Página1)

de controversia tiene una lectura evidente, que no es otra que la de augurarles una más que previsible larga estabilidad, lo que redundará y fomentará una mejor aplicación de la norma, y una más rica y detenida jurisprudencia sobre su contenido.

Por el contrario, el escaso debate sobre el contenido específico de las diligencias de investigación electrónica, se vio compensado por el que hubo sobre otros aspectos procesales ya enunciados más arriba[274]. En cambio, no se debatió sobre aspectos esenciales de estas diligencias, como son: su origen, sus resultados en la experiencia comparada de otros ordenamientos jurídicos que lleven aplicándola más tiempo que el nuestro, los problemas que se han suscitado en su práctica en los ordenamientos extranjeros, y en general se echó en falta un debate sosegado y minucioso sobre las posibilidades y consecuencias sobre el proceso penal de la instauración de estas nuevas diligencias tecnológicas.

Los grupos parlamentarios sí que coincidieron en la necesidad de actualizar la Ley de Enjuiciamiento Criminal, y en la perentoriedad de renovar las diligencias de investigación vigentes, y coincidieron en la necesidad de crear nuevas medidas de investigación, adaptadas al nuevo contexto social y cultural, marcado por el uso intensivo de las nuevas tecnologías de la información y de la comunicación, también aplicadas a los actuales comportamientos delictivos.

En cuanto al concreto contenido propuesto, durante el debate de las diligencias de acceso a dispositivos de almacenamiento masivo de datos y acceso remotos a equipos informáticos, son escasas las modificaciones propuestas por los distintos grupos parlamentarios en relación al Proyecto de Ley presentado por el Gobierno. En este sentido, se puede destacar que no se presentó ninguna propuesta que rechazase frontalmente la regulación propuesta[275].

---

[274] Hay que destacar que el hecho de que en un mismo debate parlamentario se analizasen dos normas con tan enorme trascendencia fue puesta de manifiesto por algún grupo parlamentario; así señor ESTEBAN BRAVO (grupo parlamentario PNV), dijo textualmente: «*Señora vicepresidenta, señoras y señores diputados, coincido con algunos de los anteriores intervinientes en que no me parece nada oportuna y desde luego no está haciendo ningún favor al parlamentarismo la dinámica de leyes por embudo a las que nos está sometiendo el grupo mayoritario. Han fijado un calendario y no sé en qué están pensando para la próxima legislatura, probablemente tienen claro que no estén en el Gobierno, y que desde luego no van a tener mayoría absoluta, y están decididos a hacer una reforma unilateral de leyes que mi grupo entiende que deberían tener un consenso amplio. Se trata además de una reforma exprés de leyes que deberían necesitar un tiempo de reposo y maduración para proceder a su modificación. Creo que se equivocan, creo que es un error, creo que están haciendo daño al parlamentarismo»*. Pág. 24-25 del Diario de Sesiones que se puede leer en el enlace ofrecido por la página web del Congreso: http://www.congreso.es/portal/page/portal/Congreso/PopUpCGI?CMD=VERLST&BASE=pu10&FMT=PUWTXDTS.fmt&DOCS=1-1&QUERY=%28DSCD-10-PL-278.CODI.%29# (Página9).

[275] http://www.congreso.es/portal/page/portal/Congreso/PopUpCGI?CMD=VERLST&BASE=pu10&FMT=PUWTXDTS.fmt&DOCS=1-1&DOCORDER=LIFO&QUERY=%28BOCG-10-A-139-2.CODI.%29# (Página1). En el enlace facilitado, que se corresponde con lo publicado en el BOCG serie A, NÚMERO 139-2, DE 29-05-2015, cve: BOCG-10-A-139-2, se pueden contemplar las diversas iniciativas de enmienda dirigidas al texto presentado por el Gobierno. Cabe destacar que a lo largo de las noventa y nueve páginas que se exponen son escasas las iniciativas tendentes a la modificación de los artículos 588 sexies apartados a hasta c, y al artículo 588 septies, apartados a hasta c. Destacan como enmiendas referentes a las diligencias de acceso a datos contenidos en dispositivos de almacenamiento masivo y de intervención remota de equipos las siguientes: en la página 27, relativa a la enmienda 38 efectuada por el Grupo

En todo caso, sí que hubo algunos intercambios de pareceres dirigidos a cuestionar al plazo de ejecución de las medidas; las consecuencias derivadas de la falta de respuesta a la petición, y la determinación de los sujetos encargados de hacerlas.

Los debates parlamentarios no fueron el único origen de la Ley que se analiza en este trabajo, sino que el objetivo inicial de los legisladores fue el de reformar, completamente, el proceso penal español. De hecho, el debate legislativo sucintamente expuesto se produjo ante la imposibilidad de afrontar una reforma más ambiciosa de todo el proceso penal, pero ante la constatación de la inexistencia de los consensos necesarios para la reforma total de la ley procesal penal, se optó por regular aquellos aspectos de la investigación, en concreto los relacionados con el uso de las nuevas tecnologías, que resultaban perentorios para el funcionamiento de la justicia en nuestro país. Por eso, no puede desconocerse que la actual regulación bebe, en gran medida, del contenido del Anteproyecto de Código Procesal Penal.

Este Anteproyecto, con trabajos previos ya realizados, contó con diferentes informes realizados por distintos órganos implicados en materia relacionada con la Justicia, como la Fiscalía General del Estado, el Consejo General del Poder Judicial, o el Consejo de Estado. Es conveniente, para entender mucho mejor el contenido de la norma actualmente vigente, examinar el parecer de estos órganos, porque si bien es cierto que el contenido de los informes que emitieron se referían a una reforma procesal diferente a la que fue finalmente aprobada, y que pretendía un mayor calado y alcance, en algunos casos, el contenido de estos informes se refirieron al contenido concreto de las dos diligencias de registro que se analizan en este trabajo. Además, es preciso reseñar y tener presente que en lo que a estas dos diligencias se refiere, el contenido del texto del Anteproyecto de Código Procesal Penal, con respecto al finalmente aprobado, tiene pocas diferencias.

Entre estos informes, cabe citar en primer lugar, el realizado por parte del Consejo General del Poder Judicial[276]. En la materia relativa a los dispositivos de almacenamiento masivo, así como en

---

Parlamentario de IU-ICV-EUiA, CHA, Izquierda plural dirigida a modificar el contenido del art. 588 sexies c, 3 y 4 a fin de determinar las consecuencias derivadas del transcurso del plazo, entendiéndose a los efectos del citado grupo que la norma debía recoger que se entendería denegada. Esta petición coincide con la apreciada en la página 53, coincidente con la enmienda 70 (pág. 69 y 70) efectuada por el Grupo Parlamentario de Catalán del mismo tenor que la anterior; también se propuso como enmienda numerada como 90 por parte del grupo parlamentario socialista una propuesta de modificación a la redacción del art, 588 septies apartado a tendente a no limitar en el futuro los posibles medios técnicos que pudieran servir para el acceso al equipo informático; la enmienda 91(pág. 71), también propuesta por el grupo parlamentario socialista pretendía una modificación del art. 588 septies apartado c que pretendía la inclusión de mayor flexibilidad en el tiempo de duración de la intervención no limitándolo a tres meses, sino a un mes prorrogables; la enmienda 101, propuesta por el Grupo parlamentario de UPYD (página 81) se dirigía a una nueva redacción del art. 588 sexies apartado c dirigida a concretar los agentes que deberían realizar la medida; la siguiente enmienda , la 102, del mismo grupo, proponía otra redacción del art. 588 septies a, solicitando una medida tanto más genérica que la concreción determinada en el precepto sometido a análisis.

[276] Puede consultarse el contenido íntegro del informe junto a los votos particulares que se dieron sobre el mismo en el siguiente enlace: http://www.poderjudicial.es/cgpj/es/Poder-Judicial/Consejo-General-del-Poder-Judicial/Actividad-del-CGPJ/Informes/Informe-al-Anteproyecto-de-Ley-Organica-de-modificacion-de-la-Ley-de-Enjuiciamiento-Criminal-

relación con la intervención remota de equipos informáticos, el órgano de gobierno del Poder Judicial puso un gran énfasis[277] en la primera de las dos diligencias citadas. Así, muestra un importante interés y preocupación acerca del modo en que su práctica puede afectar a aquellas personas obligadas a guardar el secreto profesional.

En lo que se refiere al registro remoto de equipos informáticos, el contenido del informe del Consejo General del Poder Judicial resulta mucho más breve y escueto, aunque señala que en algunas cuestiones sobre esta diligencia se hace necesaria una mayor concreción. Es de destacar que se trata de un extensísimo informe, que se detiene mucho más en otros aspectos contemplados por el proyecto de norma, pero en cuanto a las diligencias que constituyen el objeto de este trabajo poco más se dice.

La Fiscalía General del Estado es otro de los organismos implicados en la administración de justicia que realizó también un informe sobre el anteproyecto de ley orgánica[278], aunque cabe decir que el texto sobre el que informó se detuvo en muchas cuestiones que no son plenamente coincidentes con la regulación que finalmente llegó a la Ley Orgánica 13/2015.

Las diferencias más importantes encontradas se aprecian en la falta de coincidencia entre la numeración que existía en el articulado del anteproyecto y la que finalmente recibió el proyecto de ley orgánica que se envió a las Cortes Generales para su debate y aprobación. Además, hay matices y cuestiones que se abordan dentro del informe que fueron acogidas y finalmente aprobadas en el texto final de la Ley. En todo caso, sí que puede destacarse que la norma que fue finalmente aprobada ha resultado ser mucho más extensa sobre algunas de las diligencias de investigación, que el texto originario del anteproyecto.

Con independencia de las diferencias en cuanto a la extensión del contenido entre la norma sometida a dictamen y la aprobada, la opinión del Ministerio Público sobre la medida de acceso a los datos contenidos en dispositivos electrónicos se puede resumir en que la Fiscalía remarca la importancia y la necesidad de regular esta concreta materia, porque afecta a varios derechos fundamentales al mismo tiempo: el derecho a la intimidad o el derecho al secreto de las comunicaciones. El Ministerio Fiscal se hace eco, en su informe, del contenido del derecho al propio entorno virtual, entendiéndolo como una conjunción de varios derechos, del que resulta el

---

para-la-agilizacion-de-la-justicia-penal—el-fortalecimiento-de-las-garantias-procesales-y-la-regulacion-de-las-medidas-de-investigacion-tecnologicas.

[277] Se puede acudir a las páginas 97 y siguientes del informe del CGPJ sobre el anteproyecto.

[278] El informe de la Fiscalía General del Estado en su integridad puede consultarse en el siguiente enlace: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/INFORME_CF_MODIFICACIÓN_LECrim_23-01-2015.pdf?idFile=7c2cd525-01bf-4cc0-864a-29dc8ee0dae9. Los aspectos relativos a las diligencias de acceso a dispositivos de almacenamiento masivo se encuentran en el punto. 5.16 del informe, página 110 y siguientes, mientras que su opinión sobre el acceso remoto a equipos se desarrolla en el punto 5.17, páginas 117 y siguientes del informe.

germen de un nuevo derecho fundamental. Y es que la Fiscalía no pierde de vista el hecho de que la actividad tecnológica en la actualidad y la interactuación de los sujetos con ella hace que se generen constantemente huellas de la actividad virtual (por ejemplo la derivada del acceso a redes sociales, chats, envío de whatssapps, visitas a páginas web o compras a través de internet). Todas estas manifestaciones virtuales de la actividad de las personas pueden ser seguidas por cualquiera, y por supuesto por el Estado, facultad que debe ser regulada con la clara finalidad de evitar, durante su ejecución, la vulneración de derechos fundamentales. Sobre este derecho en particular, la Circular de la Fiscalía General del Estado 1/2019, de 6 de marzo ha dedicado un apartado a su concurrencia en las diligencias reguladas en el Título VIII de la LECrim.

El Ministerio Público reseña en su informe, como elemento destacable, la importante diferencia que debe darse entre la autorización necesaria para acceder a los dispositivos de almacenamiento masivo y la que sirve para acceder al domicilio del investigado. La posición que en la actualidad mantiene la Fiscalía es que, a diferencia de otras épocas en las que consideró que con el auto que habilita el acceso al domicilio se permitía, a la vez, incautar y registrar el contenido de bienes o dispositivos relacionados con el delito investigado, se ha pasado a otra postura completamente diferente. La interpretación que permitía dicho acceso a los dispositivos sólo con la habilitación de entrada al domicilio no respetaba, a juicio de la Fiscalía, el contenido de los derechos fundamentales implicados en cada uno de esos actos.

El informe de la Fiscalía destacaba que a falta de autorización expresa por parte del investigado a los agentes, que acceden al domicilio, para que por parte de éstos se pudiera consultar el contenido de estos dispositivos electrónicos se requería la expresa autorización judicial que la sustituyese. Esta opinión de la Fiscalía, se mantiene fundada también en múltiples pareceres judiciales, que vienen a considerar que, los datos alojados en los dispositivos que se encuentren en una entrada y registro domiciliario, gozan de autonomía propia, y al estar amparados por derechos fundamentales como la intimidad, el honor, la propia imagen o el secreto de las comunicaciones, justifican que sobre todo lo que tenga que ver con ellos se produzca un pronunciamiento y una justificación judicial separadas de la habilitación de acceso al domicilio. Este mismo fundamento es de aplicación aun cuando los dispositivos sean encontrados fuera del domicilio del investigado.

En cuanto al contenido de la diligencia de acceso remoto a equipos informáticos, el informe del organismo que representa al Ministerio Fiscal remarca, como los de otros informantes de la norma, la novedad y necesidad de esta diligencia. También se alude a la existencia de una figura similar en otras legislaciones europeas, enfatizando principalmente que se trata de una diligencia que debe contemplarse con carácter restrictivo y excepcional, por lo que se considera que se trata de una medida adecuada sólo para investigar concretas infracciones penales de gravedad.

La Ley que reforma la LECrim también fue informada por parte del Consejo de Estado[279]. Este órgano desgrana la tramitación seguida por el Anteproyecto de Código Procesal al que antes se hizo alusión, destacando también algunos aspectos llamativos. De entre estos aspectos destaca el Consejo que no se haya llamado a realizar alguna propuesta a la Agencia de Protección de Datos, o a otros organismos del sector de las comunicaciones, sobre todo teniendo presente que se trataba de una reforma de la LECrim que está muy relacionada con el derecho al secreto de las comunicaciones, además de con otros derechos del art. 18 de la CE [280], lo que hubiera justificado acudir al parecer de las entidades encargadas de velar por la protección de los datos personales de los ciudadanos, y poder conocer su postura sobre la implicación de los datos que están obligados a tutelar y poner en relación dicho parecer con el ámbito penal. Se incurre, a juicio del Consejo de Estado, en una distinción innecesaria en medidas que afectan al mismo derecho con diferente alcance. La mayor preocupación del Consejo de Estado es la limitación que puede producirse en los derechos de terceras personas que compartan el dispositivo intervenido con el investigado[281] , y que puede ver como sus datos virtuales pueden salir a la luz en el curso de la investigación criminal.

El Consejo General de la Abogacía Española es otro de los organismos que también emitió varios informes relacionados con la posible afectación de los derechos contenidos en el art. 18 CE. Así, consta la presentación de un informe relativo a la entrada y registro en despachos de abogados[282] (y su consiguiente relevancia para con el secreto profesional que los abogados han de cumplir), y también se redactó otro informe, pero exclusivamente dirigido al proyecto de Ley Orgánica que es objeto de este trabajo[283]. El contenido del informe redactado con ocasión de la ley orgánica no se

[279] Puede consultarse el contenido integro del informe del Consejo de Estado en la publicación efectuada en el Boletín Oficial del Estado, que se encontrará en el enlace http://www.boe.es/buscar/doc.php?id=CE-D-2015-97

[280] Dice el informe del Consejo de Estado: «*El Anteproyecto no ha sido, sin embargo, informado por la Agencia Española de Protección de Datos, ni por la Secretaría de Estado de las Telecomunicaciones y para la Sociedad de la Información, como parecería pertinente en razón de la naturaleza de las medidas de investigación tecnológicas que regula»*.

[281] Sobre este aspecto particular el Consejo de Estado pone de manifiesto que: «*Sin embargo, el resto de medidas también podrán afectar a personas diferentes del sospechoso, aunque el Anteproyecto no lo diga: tal sucederá con toda probabilidad en la interceptación de las comunicaciones postales, del mismo modo que no es infrecuente que en un registro de papeles, un registro de dispositivos de almacenamiento masivo de información o un registro remoto de archivos informáticos se venga en conocimiento de informaciones referentes a terceros. Por tal razón, la legitimidad de las medidas de investigación del sujeto sospechoso no puede verse en entredicho por el hecho de que, mediante las mismas, pueda accederse a informaciones de terceras personas, dado que tal circunstancia es consustancial a su puesta en práctica, y así debería preverse con un alcance general para todas ellas, del mismo modo que tendría que contemplarse con el mismo alcance que las informaciones atinentes a tales personas no deberán ser incorporadas a la causa cuando no guarden relación con los fines de la investigación penal y, en especial, cuanto afecten a "la vida íntima de las personas (artículo 588 bis l.1 de la LECr»)».*

[282] El informe 8/2015 expone de forma exhaustiva, en las páginas 85 y siguientes de la compilación de informes de 2015, la opinión del Consejo de la Abogacía Española sobre la entrada y registro en Despachos de Abogados. Puede leerse el informe en el siguiente enlace: http://www.abogacia.es/wp-content/uploads/2016/02/Informes-Comision-Juridica-2015-INDICES-OK.pdf

[283] El Consejo General de la Abogacía Española emitió informe sobre la norma con número de registro RS- 04934 de fecha 27-04-2015. El enlace que puede consultarse es el siguiente: https://www.icasal.com/19969/activos/texto/wicas_test2_pdf_19969-3P9w7J6fAEiEIfkW.pdf.

refiere, en ningún momento, a las diligencias de investigación electrónica sobre las que se centra este estudio, ni con carácter general, ni tampoco con respecto a ninguna diligencia en concreto. El informe, en cambio, se detiene más en otros aspectos en los que la participación del abogado resulta más necesaria, tales como el acto de la detención, la entrevista con el detenido, su posición ante la incomunicación, la participación del letrado en concretas diligencias con el detenido, etc.

Por último, en lo que a la existencia de informes se refiere, puede decirse que existen otros realizados por organismos tales como el Defensor del Pueblo[284], si bien también en este caso, como en el del Consejo General de la Abogacía Española, tampoco se hace ninguna alusión al contenido de las diligencias de investigación electrónicas que se tratan de forma concreta en este trabajo.

En resumen, puede decirse de todo lo que se ha visto hasta el momento, recogiendo los pareceres emitidos por los agentes implicados en la reforma de la LECrim, que las opiniones vertidas sobre el contenido de la reforma concitaron un acuerdo importante en lo que se refería a la necesidad de regular concretas diligencias de investigación tecnológica que permitiesen el acceso y registro de datos albergados dentro de dispositivos electrónicos, sea de manera física o mediante accesos remotos. Se trataba, en ambos casos, de dos diligencias que han sido escasamente criticadas, tanto por los legisladores, como por los distintos organismos encargados de informar sobre la ley.

Esta ausencia de críticas dignas de mención permite desprender que se trata de diligencias que han generado mucho menos interés, debate y polémica que otras, lo que se explica por la coincidencia de los legisladores, los informantes y los operadores jurídicos, en el hecho de su necesaria inclusión en un texto legal sobre la materia. Este acuerdo generalizado se ve reforzado, en cierto modo, por la suscripción de un convenio de ámbito internacional, suscrito por España, y que se verá más adelante, que exigía su incorporación al derecho nacional interno. Todo lo anterior permite esperar, en lo que se refiere a estas dos diligencias de investigación, un cierto grado de estabilidad y perdurabilidad de la norma actual sobre estas concretas materias.

1.2. Las diligencias de investigación tecnológica en nuestro entorno geográfico y cultural: la Unión Europea e Iberoamérica.

[284] Puede consultarse el informe del Defensor del Pueblo español en el siguiente enlace: https://www.defensordelpueblo.es/resoluciones/reforma-de-la-ley-de-enjuiciamiento-criminal-6/. Cabe poner de manifiesto que el citado informe no cuenta con relevancia a los efectos de este estudio por cuanto no se pronuncia sobre las cuestiones que guardan relación con las medidas de investigación tecnológica.

Una vez que se ha terminado de analizar cuál ha sido el proceso que ha seguido la formulación de la normativa procesal española, antes de su aprobación, es momento de analizar si hay leyes de nuestro entorno, sobre esta misma materia, que influyeron, de alguna manera en la génesis de la reforma de la LECrim, en especial, en lo referido a las diligencias de acceso y registro electrónico de información.

La influencia sobre la normativa nacional ha de buscarse en las normas dictadas por países e instituciones con los que España guarda una especial relación, como son el resto de países europeos, las instituciones comunitarias a las que España pertenece, o las normas de países iberoamericanos a los que nos une una clara vinculación cultural.

Dentro del ámbito de los países europeos que se integran, con España, dentro de la Unión Europea, se van a analizar la normativa existente sobre esta materia en Alemania, Francia, Italia y Portugal. Las razones de esta elección son principalmente las de proximidad geográfica y las de influencia normativa que estos países tienen dentro del contexto europeo.

En primer lugar, y comenzando por la normativa alemana, puede destacarse que la misma siempre ha influido, tradicionalmente, en muchas de las normas penales españolas. En la materia que nos ocupa, la legislación procesal alemana permite el acceso a datos, usando para ello medios mecánicos.

Este acceso a los datos mediante el empleo de sistemas mecánicos, que no se enumeran, ni tampoco se explican en la ley alemana se permite en la investigación de determinados ilícitos penales graves [285]: por ejemplo, los relativos al tráfico de estupefacientes y armas, la falsificación de moneda y efectos timbrados, en los relativos a la protección del Estado, los delitos peligrosos para la comunidad, los delitos contra la integridad corporal, la vida, la libertad sexual o personal, la libertad comercial o aquellos delitos organizados por un faccioso[286].

[285] Vid. EIRANOVA ENCINAS, Emilio. *Código penal alemán, StGB Código Procesal Penal alemán StPO*. Marcial Pons. Madrid. 2000. Páginas 250 a 259. Es de destacar que en la sección octava relativa a la «*confiscación , supervisión de la telecomunicación, búsqueda de la trama, empleo de medios técnicos, empleo de inquisidores clandestinos y registros»*, el artículo 94 parte de la posibilidad de que puedan servir como prueba los objetos de una persona, que puede entregarlos voluntariamente o bien no hacerlo, siendo en este último caso objeto de confiscación. En todo caso las comunicaciones escritas, las anotaciones y pruebas médicas que obren en poder del investigado pueden negarse a su aportación, pero se puede pedir su confiscación. Esta confiscación sólo puede ser ordenada por un juez, y admite la norma que lo haga un funcionario (sin detallar de qué clase debe ser este funcionario), pero en todo caso debe ser confirmada por el Juez, como más tarde, en el plazo de tres días. Son en concreto los arts. 98 a y 98 b los que contienen mayores analogías con la posibilidad de acceso al contenido o los datos empleando medios mecánicos, si bien no se dice expresamente si se trata de un ordenador o de un dispositivo susceptible de almacenamiento masivo de información, aunque debe entenderse que así ha de ser, si para su extracción ha de emplearse alguna clase de mecanismo para llevarlo a la práctica.

[286] El diccionario de la RAE define como primera acepción de faccioso: «*1. adj. Dicho especialmente de un rebelde armado: que pertenece a una facción»*.

La ley procesal alemana contiene en el Capítulo VIII, en sus artículos 94 a 111p, todo un conjunto de medidas que tienen que ver con la intervención de comunicaciones, búsqueda de datos mediante el empleo de ordenadores, uso de dispositivos electrónicos, y búsqueda encubierta. En la norma germana se permite que el acceso lo acuerde un funcionario o la propia fiscalía, si bien una vez verificado, debe ser ratificado por el Juez. Esta facultad de atribuir la decisión de urgencia a un sujeto distinto del Juez, pero con la obligatoriedad de que se produzca necesariamente su ratificación posterior, es una constante que se da en las demás normas procesales europeas, como veremos, y que ha llegado también, en algunos casos a la norma española. En todo caso, esta posibilidad de la medida sin intervención inicial del Juez, que se encuentra prevista incluida en la normativa española, ha sido la que ha levantado más dudas, suspicacias, y críticas durante la tramitación parlamentaria de la Ley, pues ha sido una constante alertar sobre la posible vulneración de derechos fundamentales que se produciría, a juicio de los críticos, si primero acontece la invasión del espacio regido por el derecho fundamental, y luego, sólo se salva esto con una ratificación del hecho limitador ya consumado.

El sistema germano también contempla otras medidas de investigación electrónica como la toma de imágenes o el examen de aparatos electrónicos conectados a la red. La ley exige, para acordar la medida de intervención en las comunicaciones o escuchas, los mismos requisitos y exigencias que se han venido exigiendo por parte de la jurisprudencia española, y que ya hemos visto en otros apartados. Se parte de la misma exigencia de justificar sobradamente la necesidad de adoptar medidas invasivas de derechos fundamentales. Para lo cual, se requieren indicios suficientes que lleven a pensar en que el sujeto investigado tiene relación con los hechos que se investigan, lo que recuerda a los principios de espacialidad, necesidad, excepcionalidad y proporcionalidad que se han analizado con anterioridad en otro apartado de este trabajo.

La presencia del ministerio fiscal, como agente habilitado para adoptar alguna de estas medidas, es fundamental en la legislación alemana. Es un habilitado directo para adoptar cualquiera de estas diligencias, si bien requiere ulterior convalidación del Juez, como pasa en otras legislaciones[287].

En el proceso penal español esta facultad le era atribuida al Fiscal en el texto del Anteproyecto de Código Procesal Penal, y se incluyó en la reforma de la LECrim de 2015 en la redacción final de alguna de las diligencias actualmente vigentes, si bien sólo en caso de emergencia o de necesidad, y con un estricto plazo de información al Juez y de ratificación de la medida adoptada.

[287] Vid. MIREILLE DELMAS MARTY y ASSOCIATION DE RECHERCHES PÉNALES EUROÉENNES (ARPE) . *Procesos penales de Europa (Alemania, Inglaterra, País de Gales, Bélgica, Francia, Italia)*. Edijus. Zaragoza, 2000. Pág. 115.

La legislación procesal francesa, que vamos a analizar en segundo lugar, contiene, dentro del Título II, del Capítulo I de su Código de procedimiento penal, una previsión legal que permite tomar del lugar del crimen «*documentos, datos informáticos u otros objetos en posesión de las personas que parezcan haber participado en el crimen o poseído elementos, informaciones u objetos relativos a los hechos incriminados»*[288]. El precepto permite considerar el escenario de la comisión del hecho con trascendencia penal, como el lugar del que se pueden tomar todos los elementos que resulten de interés y utilidad para esclarecer el hecho investigado. La enumeración de los tipos de elementos que se pueden tomar del lugar de comisión del delito se realiza con amplitud, admitiéndose la posibilidad de tomar de dicho lugar un dato informático o cualquier otra cosa.

El dato informático, como indicio a usar en la investigación de delitos, cuenta con una disposición específica que desarrolla el modo en que se debe proceder a su inclusión en la investigación, aunque como puede verse no cuenta con una especial protección, en contraste con la legislación nacional. A tenor de las normas francesas «*se procederá a la incautación de los datos informáticos necesarios para hallar la verdad situando bajo custodia de la justicia bien el soporte físico de dichos datos, bien una copia realizada en presencia de las personas que han asistido a la diligencia»,* sobre la que sigue diciendo, «*Si se hubiera realizado una copia, podrá procederse, siguiendo las instrucciones del fiscal, al borrado definitivo, del soporte físico que no haya sido colocado bajo custodia de la justicia, de los datos informáticos cuya tenencia o uso sea ilegal o peligroso para la seguridad de las personas o de los bienes»*[289].

Lo destacable es que el precepto aludido permite, con esta redacción, tomar del escenario del delito los datos de un dispositivo electrónico. No se dice nada sobre el lugar en el que se encuentra ese dispositivo, como sí se dice en la legislación española. El artículo también faculta, una vez recabado el dispositivo, para realizar una copia que contenga los datos informáticos de interés para la causa y permite borrar los datos del dispositivo de origen, lo que convierte en fuente de prueba a la copia obtenida, al desaparecer la fuente originaria, tras su borrado, que en todo caso no parece de obligada ejecución.

En la legislación gala encontramos algunos otros preceptos referidos de forma específica a los datos informáticos. En concreto a la incautación de los datos, la entrega a la Justicia de los mismos, y del examen de los datos conseguidos en la investigación por parte del Juez. También hay normas sobre

[288] Artículo 56.1 del Código procesal penal francés. Se ha tomado la traducción ofrecida por el servicio de la Biblioteca de la Universidad de Salamanca. Se puede consultar en el siguiente enlace: http://diarium.usal.es/vito/2015/02/03/traducciones-al-espanol-del-derecho-frances-en-legifrance/.
[289] Se trata de los párrafos 5 y 6 del mismo artículo 56 ya mencionado en la nota anterior, extraídos de del Código Procesal Penal del año 2005.

la orden judicial relativa al borrado de los datos[290]. Por su parte, son otros los preceptos que se dedican a la posibilidad de intervenir las comunicaciones, las cuales, al igual que en otros países del entorno europeo, se circunscriben a delitos muy concretos (específicamente los castigados con pena de prisión igual o superior a dos años, cosa que contrasta con algunos supuestos de la legislación española), limitándose la duración temporal, y estableciéndose el sistema en que deben hacerse constar las conversaciones obtenidas[291].

En tercer lugar, y en lo que se refiere a la legislación de Italia, el «*Codice di procedura penale»,* contiene, a partir de los arts. 266 y siguientes, las disposiciones sobre intervención de las conversaciones y comunicaciones[292].

Estos preceptos limitan esta facultad de intervención a determinados delitos entre los que se encuentran los de tráfico de estupefacientes, tenencia de armas y de explosivos, contrabando, algunos relativos al patrimonio de las personas, entre otros. Por su parte, el art. 266 bis, permite la intervención de comunicaciones informáticas y telemáticas[293], haciendo referencia expresa a la clase de delitos para los que está permitido realizar esta diligencia, que son los mismos tipos que los que se enumeran en el art. 266, pero se extienden a los delitos que se cometen mediante el empleo de tecnología informática o telemática. Esa misma variable también existe en nuestro texto legal, y como puede verse, la admisión de diligencias de investigación electrónica, de alto grado de invasión en derechos fundamentales, queda limitada, en lógica aplicación de una regla de proporcionalidad, a los delitos más graves, entendidos éstos tanto por la pena de prisión que implican, como por la alarma social que generan[294].

La norma italiana contempla también una diligencia de interceptación del flujo de comunicación relativo a un sistema informático o a más de uno, es decir, permite intervenir cualquier mecanismo de comunicación entre dos dispositivos. Esta amplitud descriptiva abarcaría una comunicación oral o bien una trasmisión de datos. Esta forma de redacción de la norma italiana facultaría a los agentes de investigación, para que procedieran a realizar la intervención en el proceso de envío de datos a la nube, lo que expresamente no se contiene en nuestro texto legal.

La norma procesal penal italiana, en los preceptos siguientes, faculta al ministerio fiscal para adoptar la diligencia mediante un decreto. Además del fiscal, también están habilitados para adoptar

[290] Artículo 96.
[291] Vid. MIREILLE DELMAS MARTY y ASSOCIATION DE RECHERCHES PÉNALES EUROÉENNES (ARPE) . Op. Cit. Pág. 300.
[292] Vid. *Codice de procedura penale*. G.Ciappichelli editore. Torino. 2005. Pág. 143.
[293] Vid. SPANGHER GIORGIO. Op. Cit, Pág. 144.
[294] Se reitera y se da por reproducido aquí el contenido mucho más extenso de la nota número 105 de este trabajo referente al Auto de 6 de abril de 2016 dictado por la AP de Tarragona (Sección 4º). Ponente: Don Javier Hernández Garcia, y la cuestión prejudicial que el mismo plantea, así como la resolución a dicha cuestión por parte de la STJUE..

alguna diligencia de investigación electrónica otros organismos de investigación. En estos casos de adopción por agentes distintos del Juez, no resulta posible el otorgamiento de la decisión limitadora sin motivación, incluso cuando deba hacerse por razones de urgencia. El decreto dictado debe ser validado por el Juez instructor[295] en todo caso.

Este mismo Capítulo IV del *Codice,* regula otros aspectos relacionados con las medidas limitadoras de derechos como lo referido a la duración de las escuchas, el empleo de la información obtenida en otro procedimiento distinto, etc. Tal y como se puede apreciar, se trata de concretos aspectos sobre los que la legislación española también se ha pronunciado.

En cuarto lugar, y sobre el contenido de la legislación portuguesa[296], cabe decir que la misma cuenta, también, con normas sobre estas materias relativas a diligencias de investigación en las que se emplea la tecnología. Sus disposiciones sobre este particular están en los arts. 187 y siguientes del Código Procesal, que es el que reúne los requisitos y los presupuestos necesarios para proceder a efectuar una intervención telefónica.

Como parece ser una constante en las demás legislaciones europeas, para poder acordar esta medida de investigación, ha de darse como presupuesto, la investigación de alguna clase de tipo penal de suficiente gravedad que lo justifique. Se citan, como ejemplos, los delitos cuya pena de prisión sea superior a tres años, los delitos de tráfico de estupefacientes, armas, explosivos y contrabando, etc. La legislación portuguesa contempla también, entre los ilícitos que se pueden investigar mediante la diligencia de intervención de las comunicaciones, las amenazas y coacciones, siempre que en su tipo objetivo, la modalidad comisiva prevista admita la realización de la conducta típica mediante el empleo de algún sistema de comunicación, como el propio precepto contempla.

Un elemento común en las distintas normas europeas es la coincidencia de todas ellas en el carácter tasado de la medida de intervención en las comunicaciones de modo general, y también en el registro de datos cuando expresamente se contempla. La coincidencia también se da en el hecho de que se admite que el Fiscal pueda acordarla, con ratificación judicial posterior, en situaciones de emergencia. Esta posibilidad de adopción no judicial se justifica porque en otros países la instrucción es una actividad propia de este órgano encargado de acusar y no del Juez, como es el caso español.

Puede destacarse también dentro del contenido de estas legislaciones, la creciente importancia que comienzan a recibir los datos informáticos. Ahora bien, también hay que decir, que ninguna de las normativas examinadas regula de manera autónoma el acceso a datos guardados en la nube, si bien,

[295] Vid. MIREILLE DELMAS MARTY y ASSOCIATION DE RECHERCHES PÉNALES EUROÉENNES (ARPE) . Op. Cit. Pág. 378.
[296] Vid. *Código de processo penal.* Coimbra. Coimbra editora. 2001. Pág. 86.

ciertas interpretaciones sobre los artículos que regulan el acceso a los datos si que permitirían incluirlo.

Del examen de las diferentes legislaciones mencionadas en este apartado, sí que puede concluirse que la ley española resulta de las más ricas tanto desde la casuística, como de la justificación y el desarrollo de cada diligencia, comprendiendo múltiples modalidades de investigación electrónica que en otras normas europeas no se detallan, sino que deben extraerse o intuirse a través de la interpretación de un enunciado bastante amplio.

Además, la legislación española sistematiza y ordena toda la materia, establece un conjunto de principios bajo los que es posible adoptar la medida, y contiene previsión de casi cualquier supuesto en los que los datos pasan de un proceso a otro. Sin embargo, por el contrario, nuestra legislación ha sido menos receptiva que las analizadas, a la idea de que la decisión sobre la realización de una diligencia, la pueda tomar un agente diferente al Juez, siendo esta renuencia a permitir esta posibilidad una consecuencia directa de la configuración de nuestro sistema acusatorio.

En otro orden de cosas, y por lo que se refiere a las legislaciones procesales penales de Iberoamérica, su examen también permite encontrar algunos ejemplos acerca de la adopción de medidas de investigación tecnológica. Estas medidas se ciñen, principalmente, a la adopción de diligencias de investigación relacionadas con los derechos a la intimidad y al secreto de las comunicaciones, etc. En lo que se refiere a la legislación Iberoamericana, las referencias serán a las leyes procesales penales de Colombia, Argentina y México

Comenzando por la legislación procesal penal de Colombia[297] , puede decirse que en la misma existen una serie de diligencias de investigación, contenidas dentro del Libro II, del Código de procedimiento penal. El Libro se denomina «*técnicas de indagación e investigación de la prueba y sistema probatorio»*. En el Capítulo II, concretamente en los arts. 213 y siguientes, hay medidas que «*no requieren autorización judicial previa para su realización»*, si bien se encuentran sometidas a un control judicial a posteriori, que analice la legalidad de la medida adoptada.

Entre las posibles medidas que se pueden adoptar destaca el contenido del art. 236[298] que, de forma amplia, permite el acceso, siempre mediante la incautación directa del equipo informático, a los

[297] Se ha consultado la Ley 906 de 2004 (agosto 31) por la cual se expide el Código de procedimiento Penal. Publicada en el Diario Oficial 45657, de 31 de agosto de 2004.

[298] El artículo dispone: Artículo 236. «*Recuperación de información dejada al navegar por internet u otros medios tecnológicos que produzcan efectos equivalentes. Cuando el fiscal tenga motivos razonablemente fundados, de acuerdo con los medios cognoscitivos previstos en este código, para inferir que el indiciado o el imputado ha estado transmitiendo información útil para la investigación que se adelanta, durante su navegación por internet u otros medios tecnológicos que produzcan efectos equivalentes, ordenará la aprehensión del computador, computadores y servidores que pueda haber utilizado, disquetes y demás medios de almacenamiento físico, para que expertos en informática forense descubran, recojan, analicen y custodien la información que recuperen. En estos casos serán*

datos que del mismo pudieran resultar necesarios para la investigación. Para ello, se establecen como requisitos que concurran los presupuestos necesarios para cualquier entrada y registro en domicilio, a los que se remite. Por lo tanto, han de reconducirse a las exigencias de esta diligencia todas las circunstancias necesarias y exigibles para llevarlo a cabo. En este sentido lo que hace la ley es, por razones de economía, remitirse a la entrada y registro, pero no admite expresamente que los artefactos encontrados en el registro de un domicilio sean analizados sin más. El precepto también limita la posibilidad de mantener el objeto incautado de manera efectiva durante un tiempo indefinido, siendo obligatoria su pronta devolución al propietario.

La legislación argentina en esta materia se centra en el «*Código Procesal Penal de la Nación»*, aprobado en el año 2014[299]. De la lectura del artículo 144[300] se desprende la habilitación para intervenir datos informáticos, e incluso parte de un sistema de almacenamiento. Esto mismo es lo que se contiene en nuestra propia legislación.

La iniciativa en la práctica de la diligencia ha de ser de parte, según se desprende del propio tenor legal. El solicitante de la practica de esta diligencia es hecho responsable del contenido que se extraiga. En todo caso, debe ser el Juez el encargado de dictar una resolución expresa sobre su concesión o sobre la denegación de la medida, la cual deberá estar suficientemente fundamentada. Cabe hacer notar que no hay alusión expresa a la figura del Ministerio Fiscal, ni a otros órganos de investigación públicos. Con esa generalidad cabe entender que les corresponde la petición tanto a estos órganos del ministerio público, como sucede en nuestro ámbito europeo, como a las acusaciones privadas.

El mismo artículo también regula la diligencia de apertura de la información encontrada dentro del dispositivo. Resulta patente que la normativa argentina se produce una cierta asimilación entre la regulación sobre la apertura de la correspondencia escrita y a la prevista para esta diligencia de marcado carácter electrónico. En la legislación argentina hay una exigencia legal expresa referente a

---

aplicables analógicamente, según la naturaleza de este acto, los criterios establecidos para los registros y allanamientos. La aprehensión de que trata este artículo se limitará exclusivamente al tiempo necesario para la captura de la información en él contenida. Inmediatamente se devolverán los equipos incautados».

[299] El código procesal penal de la Nación fue aprobado por la ley 27063 y promulgado según el decreto 2321/2014. Puede consultarse el texto íntegro en la página del Ministerio Fiscal argentino el siguiente enlace: http://www.mpf.gob.ar/cppn/files/2015/05/Codigo_procesal_digital.pdf.

[300] Dispone el precepto que: *«ARTÍCULO 144.- Incautación de datos. El juez podrá ordenar a requerimiento de parte y por auto fundado, el registro de un sistema informático o de una parte de éste, o de un medio de almacenamiento de datos informáticos o electrónicos, con el objeto de secuestrar los componentes del sistema, obtener copia o preservar datos o elementos de interés para la investigación, bajo las condiciones establecidas en el artículo 129. Regirán las mismas limitaciones dispuestas para el secuestro de documentos. El examen de los objetos, documentos o el resultado de la interceptación de comunicaciones, se hará bajo la responsabilidad de la parte que lo solicitó. Una vez secuestrados los componentes del sistema, u obtenida la copia de los datos, se aplicarán las reglas de apertura y examen de correspondencia. Se dispondrá la devolución de los componentes que no tuvieran relación con el proceso y se procederá a la destrucción de las copias de los datos. El interesado podrá recurrir al juez para obtener la devolución de los componentes o la destrucción de los datos».*

la necesidad de destruir los datos recabados durante el registro de los dispositivos, cuando estos no resulten de interés para la causa, lo que se convierte en un modo apropiado de salvaguardar los datos de terceros, como sucede en España.

En tercer lugar, la legislación procesal penal de México[301] sobre esta materia, es la que parece la más completa comparada con otras legislaciones de su entorno geográfico inmediato. El contenido fundamental está en los artículos 291[302], 294[303] y 303[304] del Código Nacional de Procedimientos Penales.

---

[301] Código Nacional de Procedimientos penales. Publicado en el Diario Oficial de la Federación de 5 de marzo de 2014, y reformada el 17 de junio de 2016. Puede consultarse el texto en el enlace siguiente: http://www.diputados.gob.mx/LeyesBiblio/pdf/CNPP_170616.pdf.

[302] Dispone: «*Artículo 291. Intervención de las comunicaciones privadas Cuando en la investigación el Ministerio Público considere necesaria la intervención de comunicaciones privadas, el Titular de la Procuraduría General de la República, o en quienes éste delegue esta facultad, así como los Procuradores de las entidades federativas, podrán solicitar al Juez federal de control competente, por cualquier medio, la autorización para practicar la intervención, expresando el objeto y necesidad de la misma. La intervención de comunicaciones privadas, abarca todo sistema de comunicación, o programas que sean resultado de la evolución tecnológica, que permitan el intercambio de datos, informaciones, audio, video, mensajes, así como archivos electrónicos que graben, conserven el contenido de las conversaciones o registren datos que identifiquen la comunicación, los cuales se pueden presentar en tiempo real.* (Los dos párrafos anteriores han sido objeto de una redacción reciente publicada en el DOF 17-06-2016).
La solicitud deberá ser resuelta por la autoridad judicial de manera inmediata, por cualquier medio que garantice su autenticidad, o en audiencia privada con la sola comparecencia del Ministerio Público, en un plazo que no exceda de las seis horas siguientes a que la haya recibido. También se requerirá autorización judicial en los casos de extracción de información, la cual consiste en la obtención de comunicaciones privadas, datos de identificación de las comunicaciones; así como la información, documentos, archivos de texto, audio, imagen o video contenidos en cualquier dispositivo, accesorio, aparato electrónico, equipo informático, aparato de almacenamiento y todo aquello que pueda contener información, incluyendo la almacenada en las plataformas o centros de datos remotos vinculados con éstos. Este párrafo también se reformó el 17 de junio de 2016,al igual que los dos primeros. *Si la resolución se registra por medios diversos al escrito, los puntos resolutivos de la autorización deberán transcribirse y entregarse al Ministerio Público. Los servidores públicos autorizados para la ejecución de la medida serán responsables de que se realice en los términos de la resolución judicial».*

[303] Dispone: «*Artículo 294. Objeto de la intervención. Podrán ser objeto de intervención las comunicaciones privadas que se realicen de forma oral, escrita, por signos, señales o mediante el empleo de aparatos eléctricos, electrónicos, mecánicos, alámbricos o inalámbricos, sistemas o equipos informáticos, así como por cualquier otro medio o forma que permita la comunicación entre uno o varios emisores y uno o varios receptores. En ningún caso se podrán autorizar intervenciones cuando se trate de materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su Defensor. El Juez podrá en cualquier momento verificar que las intervenciones sean realizadas en los términos autorizados y, en caso de incumplimiento, decretar su revocación parcial o total».*

[304] Dispone: «*Artículo 303. Localización geográfica en tiempo real y solicitud de entrega de datos conservados. Cuando el Ministerio Público considere necesaria la localización geográfica en tiempo real o entrega de datos conservados por los concesionarios de telecomunicaciones, los autorizados o proveedores de servicios de aplicaciones y contenidos de los equipos de comunicación móvil asociados a una línea que se encuentra relacionada con los hechos que se investigan, el Procurador, o el servidor público en quien se delegue la facultad, podrá solicitar al Juez de control del fuero correspondiente en su caso, por cualquier medio, requiera a los concesionarios de telecomunicaciones, los autorizados o proveedores de servicios de aplicaciones y contenidos, para que proporcionen con la oportunidad y suficiencia necesaria a la autoridad investigadora, la información solicitada para el inmediato desahogo de dichos actos de investigación. Los datos conservados a que refiere este párrafo se destruirán en caso de que no constituyan medio de prueba idóneo o pertinente. En la solicitud se expresarán los equipos de comunicación móvil relacionados con los hechos que se investigan, señalando los motivos e indicios que sustentan la necesidad de la localización geográfica en tiempo real o la entrega de los datos conservados, su duración y, en su caso, la denominación de la empresa autorizada o proveedora del servicio de telecomunicaciones a través del cual se operan las líneas, números o aparatos que serán objeto de la medida. La petición deberá ser resuelta por la autoridad judicial de manera inmediata por cualquier medio que garantice su autenticidad, o en audiencia privada con la sola comparecencia del Ministerio Público. Si la resolución se emite o registra por medios diversos al escrito, los puntos*

Esta legislación otorga más importancia a la regulación de las intervenciones de las comunicaciones, que hace extensiva a los datos derivados de las mismas, que a otras diligencias de investigación electrónica. Es una constante en las legislaciones consultadas el hecho de partir de la intervención de las comunicaciones, y sobre esta diligencia hacer pivotar el resto de posibles diligencias relacionadas con la toma de datos, etc. Comparada la legislación mexicana con la española, puede decirse que la nuestra legislación cuenta con una regulación específica sobre el contenido de los datos informáticos, y el modo de acceso a los mismos, de lo que carece la legislación mexicana, lo que permite abundar nuevamente en la idea de riqueza y sistematización que puede predicarse de la legislación nacional.

La práctica de las diligencias de intervención de las comunicaciones están vedadas para la investigación de una serie de conductas delictivas, lo que se muestra como una constante en todas las legislaciones consultadas, que prescinden de medidas limitativas de derechos fundamentales en casos penales de escasa relevancia, si bien es cierto que las intervenciones telefónicas constituyen un valioso mecanismo de investigación del que podría prescindirse, prematuramente, ante la configuración inicial de los hechos.

En relación con los datos obtenidos de la práctica de estas medidas de intervención de comunicaciones, su incorporación al acervo probatorio del proceso, sólo se incluyen si estos datos forman parte de alguna clase de intercambio de comunicaciones, lo que excluiría la inclusión de los datos que resultaran ajenos a ese proceso comunicativo, salvo que se realizara una interpretación amplia y extensiva del concepto de comunicación, que la ley ni admite ni rechaza. En todo caso la

---

resolutivos de la orden deberán transcribirse y entregarse al Ministerio Público. En caso de que el Juez de control niegue la orden de localización geográfica en tiempo real o la entrega de los datos conservados, el Ministerio Público podrá subsanar las deficiencias y solicitar nuevamente la orden o podrá apelar la decisión. En este caso la apelación debe ser resuelta en un plazo no mayor de doce horas a partir de que se interponga. Excepcionalmente, cuando esté en peligro la integridad física o la vida de una persona o se encuentre en riesgo el objeto del delito, así como en hechos relacionados con la privación ilegal de la libertad, secuestro, extorsión o delincuencia organizada, el Procurador, o el servidor público en quien se delegue la facultad, bajo su más estricta responsabilidad, ordenará directamente la localización geográfica en tiempo real o la entrega de los datos conservados a los concesionarios de telecomunicaciones, los autorizados o proveedores de servicios de aplicaciones y contenidos, quienes deberán atenderla de inmediato y con la suficiencia necesaria. A partir de que se haya cumplimentado el requerimiento, el Ministerio Público deberá informar al Juez de control competente por cualquier medio que garantice su autenticidad, dentro del plazo de cuarenta y ocho horas, a efecto de que ratifique parcial o totalmente de manera inmediata la subsistencia de la medida, sin perjuicio de que el Ministerio Público continúe con su actuación. Cuando el Juez de control no ratifique la medida a que hace referencia el párrafo anterior, la información obtenida no podrá ser incorporada al procedimiento penal. Asimismo el Procurador, o el servidor público en quien se delegue la facultad podrá requerir a los sujetos obligados que establece la Ley Federal de Telecomunicaciones y Radiodifusión, la conservación inmediata de datos contenidos en redes, sistemas o equipos de informática, hasta por un tiempo máximo de noventa días, lo cual deberá realizarse de forma inmediata. La solicitud y entrega de los datos contenidos en redes, sistemas o equipos de informática se llevará a cabo de conformidad por lo previsto por este artículo. Lo anterior sin menoscabo de las obligaciones previstas en materia de conservación de información para las concesionarias y autorizados de telecomunicaciones en términos del artículo 190, fracción II de la Ley Federal de Telecomunicaciones y Radiodifusión»".

amplitud con la que los datos se describen en la ley permitiría la incorporación al proceso de cualquier clase de intercambio de datos.

La legislación mexicana, de forma distinta a las legislaciones de su entorno, amplía el concepto de receptáculo de datos, considerando como tal, cualquier clase de dispositivo en el que los mismos pudieran encontrarse. Por ese mero hecho, el artefacto se considera apto para ser registrado. La legislación española sigue una versión muy parecida, en el sentido de admitir el registro de cualquier dispositivo que permita guardar o contener datos.

El contenido del artículo 291 del Código Nacional también es susceptible de ser reseñado. Es un precepto que contempla expresamente la posibilidad de que los datos de interés para la investigación criminal estén almacenados en servidores remotos. Esta expresión, ofrece una gran ventaja desde el punto de vista de la seguridad jurídica que se concede a la medida. Es decir, contra la fórmula elegida en nuestra legislación, que contempla el acceso como una forma complementaria a un registro previo, y que adolece de la falta de claridad y de precisión deseable en una norma tan reciente, la legislación mejicana permite directamente el acceso a servidores remotos. Esto se hace de forma categórica, simple y expresa, si bien es cierto que se ignoran las repercusiones y limitaciones existentes en materia de competencia territorial, que no se analizan, en lo que se refiere a la legislación mexicana, en este estudio.

En resumen, puede decirse que destaca una creciente preocupación de los diferentes Estados nacionales por combatir la comisión de todo tipo de actos delictivos que se realizan aprovechando las ventajas que ofrecen las nuevas tecnologías. En todas las legislaciones que se han analizado existe, con mayor o menor detalle, una modalidad de investigación fundamental, que es la intervención de comunicaciones y sobre ella se ha ido ampliando el concepto de registro de datos.

Otro aspecto a destacar es el hecho de que la mayor parte de los ordenamientos analizados hayan ido progresivamente reconociendo el protagonismo que en las modernas investigaciones criminales ocupa la diligencia de intervención de los datos electrónicos, estén asociados a un proceso de comunicación, o se obtengan de manera autónoma.

En buena parte de las legislaciones, según el ámbito geográfico, aunque con bastante coincidencia en general, el Ministerio Público resulta facultado para acordar esta medida con independencia de que el Juez pueda hacerlo, sobre todo en casos de urgencia. En todo caso, en la mayor parte de ellos, si no en todos, no se prescinde del papel del Juez, quien, o bien ratificará la medida adoptada previamente, o bien será el encargado de decidir sobre ella directamente. Por último, hay que destacar también una preocupación importante por el contenido de los datos. Dado que en la mayor parte de los casos también existen normas en las que se dispone la eliminación de los datos que no guarden interés para la causa, así como la destrucción de los mismos.

En conclusión, cabe decir que dentro del ámbito de las legislaciones nacionales existe una cada vez mayor presencia de diligencias de investigación electrónica, aunque queda aún un notable esfuerzo armonizador para facilitar la investigación de los delitos transfronterizos fuera del marco de la cooperación de la Unión Europea.

1.3. Las diligencias de investigación tecnológica en la legislación internacional.

El tercero de los focos de influencia que pueden ser considerados como antecedentes, siquiera remotos, de la normativa española sobre las diligencias de investigación tecnológica, se encuentra dentro del ámbito de la legislación internacional. En concreto, hemos de analizar el contenido de algunos de los más importantes tratados suscritos sobre delincuencia tecnológica, que actuaron como verdaderos precursores de la ley finalmente promulgada.

La Exposición de Motivos de la Ley Orgánica 13/2015, contiene algunas alusiones a normas internacionales que se han tenido presentes en la redacción de la normativa aprobada[305]. Entre otros, se refiere de forma expresa al Convenio sobre Ciberdelincuencia, de 23 de noviembre de 2001, ratificado por España el 20 de mayo de 2010.

Este Convenio fue suscrito en el ámbito del Consejo de Europa[306], y devino derecho interno tras su publicación en el Boletín Oficial del Estado[307] . De su contenido destaca la preocupación de los países firmantes sobre la «*protección frente a la ciberdelincuencia…conscientes de los profundos cambios provocados por la digitalización, la convergencia y la globalización continuas de las redes informáticas»*.

Los Estados firmantes son cada vez más sensibles sobre el uso, cada vez más frecuente, de los datos «*para cometer delitos y de que las pruebas de relativas a dichos delitos sean almacenadas y transmitidas por medio de dichas redes*". Ante esta realidad, la finalidad que se le da a este instrumento internacional es, «*prevenir los actos que pongan en peligro la confidencialidad, la*

[305] El apartado IV de la Exposición de Motivos alude al «*artículo 16 del Convenio sobre Ciberdelincuencia, de 23 de noviembre de 2001, ratificado por España el 20 de mayo de 2010»*, aunque haciendo referencia a la orden de conservación de los datos.

[306] A efectos de no incurrir en dudas acerca del organismo en cuestión puede consultarse el enlace: https://www.coe.int/en/web/commissioner. Debe considerarse al organismo como una organización de Estados europeos cuyo objetivo es desarrollar principios democráticos comunes entre sus miembros, basándose en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales y otros estándares sobre derechos humanos. El CdE, fundado en 1949, tiene su sede en Estrasburgo, Francia (definición ofrecida por https://www.crin.org/es/guias/onu-sistema-internacional/mecanismos-regionales/consejo-de-europa).

[307] La publicación del Convenio sobre la Ciberdelincuencia se hizo en el BOE de 17 de diciembre de 2010. Se puede consultar el enlace: https://www.boe.es/boe/dias/2010/09/17/pdfs/BOE-A-2010-14221.pdf.

integridad y la disponibilidad de los sistemas, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos…»[308].

El Convenio trata de evitar el mal uso de los datos, la ocultación de estos para fines delictivos, y la posibilidad de que los Estados, a través del empleo de los medios de investigación pertinentes, puedan acudir al uso de mecanismos de investigación que les permitan hacerse con esos datos con el fin de impedir la comisión de delitos. Se trata, por lo tanto, de otorgarse mutuamente, un conjunto de normas comunes para que, tras su incorporación al ordenamiento de cada Estado se actúe de forma conjunta, similar y ordenada contra situaciones que antes quedaban huérfanas de previsión legal.

Por contra, los valores de las sociedades democráticas sólo admiten este acceso tratando de «*garantizar el debido equilibrio entre los intereses de la acción penal el respeto a los derechos fundamentales consagrados en el Convenio del Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades Fundamentales (1950), el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (1966) y otros tratados internacionales aplicables en materias de derechos humanos, que reafirman el derecho a defender la propia opinión sin interferencia..la libertad de expresión, incluida la libertad de buscar, obtener y comunicar información e ideas .....así como el respeto a la vida privada»*". Es decir, se trata de conjugar la protección de los derechos fundamentales, con la protección a los ciudadanos, evitando el mal uso de los datos, y la comisión de delitos mediante su uso y empleo. El Consejo también tuvo presente el acervo normativo anterior al dictar el texto finalmente aprobado en Budapest el 23 de noviembre de 2001[309].

El Convenio suscrito cuenta con un preámbulo, seguido de cuarenta y ocho artículos distribuidos en cuatro capítulos denominados del siguiente modo: el primer capítulo se denomina Terminología (art.1); el Capítulo segundo se denomina de las Medidas que deberán adoptarse a nivel nacional (arts. 2 a 22), y se distribuye, a su vez, en tres secciones llamadas Derecho penal sustantivo, Derecho Procesal y Jurisdicción; a su vez, la primera de estas tres secciones se subdivide en cinco títulos: delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos; delitos informáticos; delitos relacionados con el contenido; delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines y otras formas de responsabilidad y

[308] Preámbulo del Convenio. Se ha estimado necesario ofrecer al lector el texto original porque su descripción resulta muy bien escrita, y transmite perfectamente al lector el objetivo que se persigue con la promulgación de este convenio.
[309] El Preámbulo del convenio cita: El convenio del Consejo de Europa de 1981 para la protección de las personas con respecto al tratamiento informatizado de datos personales; la Convención de Derechos del Niño de las Naciones Unidas (1989), el Convenio sobre las peores formas de trabajo infantil de la Organización Internacional del Trabajo (1999), Tratados del Consejo de Europa sobre cooperación en materia penal.

sanciones; Cooperación internacional (arts. 23 a 35), con una sección dedicada a principios generales, y la segunda dedicada a disposiciones especiales.

El Capítulo tercero se denomina de la Cooperación internacional, y se subdivide en dos secciones, la primera sección consta de cuatro títulos: principios generales relativos a la cooperación internacional, principios relativos a la extradición, principios generales relativos a la asistencia mutua y procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables.

La segunda Sección consta de tres títulos denominados respectivamente, asistencia mutua en materia de medidas provisionales, asistencia mutua en relación con los poderes de investigación y Red 24/7; el último capítulo se refiere a Disposiciones finales (arts. 36 a 48).

Del contenido de todo el Convenio, lo más relacionado con las diligencias que constituyen el objeto de este trabajo son el art. 1, y los artículos 14 y siguientes. El primero de los artículos mencionados recoge una serie de definiciones que otorgan un significado común a toda una serie de expresiones. Se trata de definir los conceptos sistema informático, dato informático[310], proveedor de servicios y datos relativos al tráfico[311]. Es un glosario muy útil y práctico para entender una materia tan compleja y desconocida para los juristas como lo es la informática. Por ello es necesario convenir cómo se debe entender cada concepto en concreto y este conjunto de definiciones cumple con esa finalidad.

La definición previa de estos conceptos básicos es un aspecto importante porque ayuda a mejorar la comprensión y la definición de algunos comportamientos típicos, entender cuáles son los bienes jurídicos que se deben proteger, y cómo ha de ser el uso de la tecnología que puede menoscabarlos, etc. También es destacable la utilidad de las menciones y definiciones relativas a sistema informático, dato informático y datos relativos al tráfico, así como la de los proveedores de servicios, porque los servicios en red también pueden integrar los servicios en "la nube", y mejorar la comprensión de este tipo de servicios on line ayuda a mejorar la concreta definición de la diligencia de registro de datos que se encuentran depositados en servicios de esta naturaleza.

Por otro lado, hay que destacar que la influencia de este Convenio en la legislación nacional es evidente, porque describe el contenido de determinadas acciones delictivas que deben incorporarse

[310] La definición que el Convenio ofrece sobre dato informático es coincidente con la que se recoge en otra legislación tenida en cuenta en la modificación del Código Penal en el año 2010 realizada mediante la promulgación de la Ley Orgánica 5/2010 de 22 de junio que modifica el Código Penal, en concreto se recogió la misma definición en el art. 1 apartado b) de la Decisión marco 2005/222/JAI del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información.

[311] No se debe olvidar que estas expresiones constituyen también derecho interno, al haber sido un Convenio convalidado por el Parlamento, y por lo tanto sirven a los efectos de explicar las expresiones enumeradas desde un punto de vista legal, de manera que las mismas se entenderán igual en todos los países firmantes del Convenio.

necesariamente a las legislaciones nacionales de los países firmantes como tipos penales. Junto a este conjunto de normas de derecho penal sustantivo, se incluyen también unas normas en materia procesal, que deben ser igualmente incorporadas a la legislación nacional de cada Estado firmante.

En particular, los artículos 7 a 10 del Convenio, definen los delitos de falsificación informática[312], el delito de fraude informático[313], los delitos relacionados con la pornografía infantil (producción con intención de difusión, oferta o puesta a disposición a través de un sistema informático, difusión a través de un sistema informático, adquisición de pornografía infantil a través de un sistema informático para uso propio o para terceros, posesión de la pornografía infantil en un sistema informático o en un sistema de almacenamiento informático)[314] y los delitos relacionados con la propiedad intelectual[315].

Los artículos 11 y 12 regulan las modalidades de ejecución en tentativa, así como la participación en complicidad, y la responsabilidad penal de las personas jurídicas. En el Código Penal español están regulados esos delitos, si bien su redacción definitiva deriva de la reforma operada en el Código Penal español en el año 2015, que es resultado de la adaptación de la legislación española a otras normas diferentes a las de este Convenio[316].

---

[312] El contenido del actual artículo 400 del CP castiga la fabricación, recepción, obtención y tenencia de programas informáticos destinados a las acciones descritas en los artículos anteriores, dedicados a la falsificación de moneda, documentos, etc.

[313] El artículo 248 del CP regula dentro del tipo básico de la estafa, en el párrafo segundo las modalidades comisivas consistentes en el empleo de manipulaciones informáticas con ánimo de obtener una transferencia económica (apartado a), y los que fabriquen, introduzcan, posean o faciliten programas informáticos destinados a comisión de estafas (apartado b). Por otro lado el artículo 264 regula los daños producidos en sistemas informáticos : acciones castigadas son el borrado, el daño, el deterioro, la alteración y la supresión o la acción de imposibilitar el acceso a los datos informáticos.

[314] En la actualidad los delitos relativos a la pornografía infantil se encuentran regulados en el art. 189 del CP, tras la redacción otorgada a los mismos por la Ley Orgánica 1/2015, de 30 de marzo.

[315] El párrafo segundo del art. 270 del CP castiga dentro de los delitos contra la propiedad intelectual la facilitación de acceso mediante mecanismos informáticos a obras protegidas mediante la propiedad intelectual, sin autorización de sus titulares de los correspondientes derechos o sus cesionarios, castigando especialmente la oferta de enlaces directos a tales obras.

[316] La Exposición de Motivos de la Ley 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 1071995, de 23 de noviembre , del Código Penal establece expresamente las distintas normas europeas en base a las que se producen determinadas modificaciones en diversos tipos penales. Expresamente dice: *«buena parte de las modificaciones llevadas a cabo están justificadas por la necesidad de atender compromisos internacionales. Así, la reforma se ocupa de la transposición de la Decisión Marco 2008/913/JAI, relativa a la lucha contra determinadas formas y manifestaciones de racismo y xenofobia mediante el Derecho Penal; de la Directiva 2009/52/CE, por la que se establecen normas mínimas sobre las sanciones y medidas aplicables a los empleadores de nacionales de terceros países en situación irregular; de la Directiva 2011/93/UE, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil; de la Directiva 2011/36/UE, relativa a la prevención y lucha contra la trata de seres humanos y a la protección de las víctimas; de la Directiva 2013/40/UE, relativa a los ataques contra los sistemas de información y la interceptación de datos electrónicos cuando no se trata de una comunicación personal; y de la Directiva 2014/42/UE, de 3 de abril, sobre el embargo y el decomiso de los instrumentos y del producto del delito en la Unión Europea. Asimismo, se modifica la actual regulación del delito de inmigración ilegal, separando claramente esta figura delictiva del delito de trata de seres humanos y ajustando tipos y penas a las exigencias derivadas de la Directiva 2002/90/CE y la Decisión Marco 2002/946/JAI»*.

En materia procesal, los artículos 14 y 15 del Convenio obligan a asumir, como derecho interno de los países suscriptores, los mecanismos de investigación de delitos que se recogen a partir del artículo 16, si bien *«resulta aplicable no solamente a los denominados delitos informáticos, sino también «a la obtención de pruebas electrónicas de cualquier delito» [art. 14.2 c) del Convenio]».* [317].

Con carácter previo a adoptar las diligencias de investigación que contiene el Convenio, y conscientes del enorme potencial invasivo en los derechos fundamentales de los ciudadanos que éstas tienen, cada país firmante debe cerciorarse de que su legislación se ajusta a las normas internacionales que salvaguardan los derechos humanos, y como parte de ello, exige que las diligencias se adapten al principio de proporcionalidad, en el modo en que ya fue explicado en otras partes de este trabajo. En aras a la contribución a una salvaguarda de los derechos que pudieran verse afectados, y para asegurar que la diligencia que se adopte resulta proporcionada a los hechos, se exige la intervención de un órgano judicial o de un órgano independiente que examine y controle tales diligencias. El Convenio requiere y exige asegurar un control de la limitación, y para ello es necesario que se reconozca el derecho fundamental afectado por la diligencia, se legisle sobre el modo de limitar dichos derechos, y se otorgue al modo de limitarlos un sistema de control que se extienda a las razones que justifican la practica, la duración y el ámbito de aplicación de la diligencia. Además, el Convenio insta a que se tengan en cuenta los intereses de terceros, sin dar mayores detalles de cómo hacer esto último, con lo que deja este aspecto en manos de cada legislación nacional.

En otro orden de materias, los artículos 16 y 17[318] se refieren a la obligación de conservación y entrega rápida de datos informáticos almacenados, así como a la imposición a terceros de estas exigencias. El articulo 16 permite que la legislación nacional imponga a cualquier tercero la obligación de conservar determinados datos informáticos, sean datos de contenido, o bien datos de tráfico, pero que en todo caso han de estar dentro de un sistema informático. Para poder imponer esta obligación a un tercero, se exige que los datos puedan perderse en el caso de no ordenarse a dicho tercero su conservación. Esta obligación de conservación está sometida a plazo, que puede alcanzar, como máximo, noventa días, durante los que el tercero los tiene que conservar obligatoriamente. Esta medida se ha adoptado en la legislación española, como ya hemos analizado en páginas anteriores, estableciéndose un lapso temporal suficiente para recabar de la autoridad

[317] Cfr. DELGADO MARTÍN, Joaquin. «Investigación del entorno virtual: el registro de dispositivos digitales tras la reforma por LO 13/2015». *Diario La Ley,* nº 86932 de febrero de 2016. LA LEY 229/2016. Pág. 2.
[318] Los artículos 16 y 17 del Convenio de Budapest son los precursores de los artículos que en nuestra LEcrim reformada en el año 2015 constituyen los artículos 588 octies que regula la conservación de los datos.

competente la habilitación para acceder a los datos de interés e imponiéndose la obligación accesoria de guardar secreto sobre la investigación desarrollada.

El articulo 17, cuya rúbrica es *«conservación y revelación parcial rápida de los datos relativos al tráfico»,* obliga a instituir los mecanismos legales necesarios para exigir la conservación de datos prevista en el precepto anterior, así como la implementación de otros instrumentos que permitan la entrega rápida de éstos datos a las autoridades que los requieran.

El artículo 18 dispone la facultad de los distintos Estados firmantes, para que, mediante sus agentes investigadores, emitan una orden, dirigida a un tercero, para que presente ante dichos agentes, los datos que se puedan tener almacenados sobre hechos que constituyen el objeto de la investigación penal. Esta orden es, por tanto, un mandato dirigido a una persona para que comunique los datos que tiene bajo su poder o control, y que los tenga almacenados en un sistema informático o en un dispositivo de almacenamiento. Es necesario que la persona concernida por la orden esté dentro del territorio (lo que comportará importantes consecuencias a efectos de la exigencia de datos alojados en la nube); además, la orden puede conllevar el deber de presentación de datos de un abonado a los proveedores que ofrezcan el servicio en el territorio (nótese que nuevamente hay en la norma una referencia territorial). En el párrafo tercero del precepto se aclara el concepto de dato de un abonado, siendo en este caso, los datos distintos a los propios de tráfico. Son los apartados a) hasta c) del artículo 18 del Convenio los que describen en qué consisten dichos datos del abonado: tipo de servicio de comunicación, identidad, dirección postal del abonado, situación geográfica, número de teléfono, etc.

El artículo 19[319] permite el registro o «*acceso de modo similar»* de un sistema informático, de una parte de este y de los datos almacenados en el mismo, así como el acceso a cualquier dispositivo de almacenamiento de datos susceptibles de contenerlos, siempre que estén en el territorio del país firmante.

Este artículo se configura como el precedente inmediato de la medida consistente en el acceso a dispositivos de almacenamiento masivo de información, así como del acceso remoto a equipos informáticos de nuestra legislación procesal. Como se ve en el contenido de la norma, es demasiado frecuente la alusión territorial, lo que conlleva algunos problemas para la investigación de dichos

[319] El informe del Consejo Fiscal al anteproyecto de Ley Orgánica de modificación de la Ley de Enjuiciamiento Criminal para la afiliación de la Justicia penal, el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, considera que el artículo 19 del Convenio es el antecedente del actual apartado de la LEcrim constituido por los arts. 588 sexies dedicados en sus apartados a hasta c a las medidas de registro de almacenamiento masivo de información. Por su parte el mismo informe considera que el párrafo 2 del art. 19 es el antecedente de la diligencia de acceso remoto a los equipos informáticos que se regulan en los arts. 588 septies a hasta c. Pág. 110 y 120. También lo considera así DELGADO MARTÍN, Joaquin. «Investigación del entorno virtual…». Op. Cit. Pág. 10.

datos, sobre todo derivados de la ubicación territorial de los mismos, y todo ello relacionado con la competencia judicial para ordenar su retención, acceso y registro.

El párrafo segundo del art. 19, permite a las autoridades encargadas de la investigación de un hecho, que amplíen el registro a otro sistema informático o a una parte del mismo, siempre que esté dentro del territorio, y que además estos datos resulten accesibles a partir del sistema inicial. La redacción que tiene la norma española es casi idéntica a la que presenta este precepto[320].

El Convenio también permite incautar un sistema informático, o una parte del mismo, o bien un dispositivo de almacenamiento de información. También permite el acceso y la conservación de una copia de esos datos, preservar su integridad y hacerlos inaccesibles. Además, también se puede interesar la ampliación del registro, siempre que existan fundadas razones, extendiéndolo a un sistema informático, pero exigiendo también en este caso, de forma clara y concisa, que el mismo se encuentre dentro del territorio nacional.

La regulación del art. 19 del Convenio se refiere al supuesto de la localización de un dispositivo que en su interior contiene datos, mientras que el contenido del art. 20 contempla otra medida que también permite el acceso a datos, pero en este segundo caso, a diferencia del anterior, se trata de un acceso a los datos de tráfico en tiempo real.

El contenido del art. 20 se complementa con el del art. 21 que se refiere a la interceptación de datos referentes no al tráfico, sino al contenido. En los dos casos los preceptos permiten que las legislaciones nacionales puedan prever medidas de investigación que permitan grabar directamente estos datos, o recibir de terceros la asistencia necesaria para hacerlo. Esta norma supuso la habilitación para recepcionar en nuestro Derecho la diligencia de registro remoto de equipos, que se verá más adelante. La legislación española contempla todas estas medidas, si bien lo hace bajo otra denominación.

El Convenio también admite el acceso a la información alojada o contenida en la nube, aunque ello se permite sólo cuando existe constancia de que el sistema donde se aloja la información está en el territorio del país firmante. Esta cuestión, que queda tan acotada en el Convenio, no está resuelta debidamente en nuestra legislación procesal, pues, como se tendrá ocasión de ver, el legislador ha pretendido dar un paso más allá en el diseño de esta medida, permitiendo el acceso y registro de datos albergados en la nube, sin hacer mención al elemento territorial previsto en el Convenio pero finalmente el texto adoptado aporta más confusión que certeza al plantear una serie de interrogantes importantes relativos a cómo habrá de practicarse esta diligencia.

[320] El contenido encaja con la redacción que en la actualidad ofrece el art. 588 sexies, apartado c , párrafo tercero de la LEcrim, tras la reforma del año 2015.

1.4. Influencia de las resoluciones judiciales en la legislación actual.

En último lugar, para terminar con este apartado, dedicado a analizar las posibles influencias que determinaron el contenido de la reforma de la LECrim en materia de diligencias de investigación tecnológica, finalmente aprobada, hay que dedicarle un espacio propio al análisis que la jurisprudencia ha tenido en la configuración del contenido de la reforma procesal en esta materia.. En especial, es destacable, el papel desempeñado por los tribunales, esencialmente el Tribunal Constitucional y el Tribunal Europeo de los Derechos Humanos en el análisis del uso de la tecnología en las investigaciones criminales y su afectación a los derechos fundamentales, así como en la configuración de la práctica concreta de las diligencias de investigación.

Hay dos sentencias que pueden ser consideradas como las más determinantes en la redacción de la legislación actual, son dos sentencias: una dictada por el Tribunal Europeo de Derechos Humanos, y otra dictada por el Tribunal Constitucional.

La Sentencia de 30 de mayo de 2017, del Tribunal Europeo de Derechos humanos, fue dictada a consecuencia de un recurso interpuesto contra una sentencia del Tribunal Supremo de España, dictada el 18 de febrero de 2009, y que más tarde fue objeto de pronunciamiento por parte del Tribunal Constitucional español, que desestimó el recurso de amparo interpuesto por el recurrente a través de su sentencia 173/2011[321], que confirmó la ausencia de intromisión ilegítima en el derecho constitucional a la intimidad.

El supuesto de hecho que se analizó por el Tribunal fue el acceso realizado a un ordenador personal por agentes de la policía sin que se contase con expreso consentimiento de su dueño. El demandante consideró que este acto efectuado por la policía fue una intromisión ilegítima en su vida privada y en su intimidad, que se había realizado sin su consentimiento expreso, y sin solicitar la necesaria autorización judicial. Se cuestionó si era aplicable la doctrina del Tribunal Constitucional conforme a la cual, en situaciones de urgencia es posible que los agentes recaben la información en cuestión, siempre que la valoración efectuada *ex post* permita concluir que se trataba de una medida razonable y proporcionada.

Sin embargo, el TEDH no consideró justificado el hecho. Parte en su análisis del Convenio Europeo de Derechos humanos, que permite excepcionar el contenido del derecho a la intimidad previsto en el art. 8 siempre que se den las circunstancias previstas en las leyes. Sin embargo, la sentencia

[321] Se trata de la STC 173/2011, de 7 de noviembre. Ponente: Don Eugenio Gay Montalvo.

consideró que no había disposición legal alguna, dentro del ordenamiento jurídico español, que habilitase a los agentes de policía para acceder al contenido de un ordenador obviando la voluntad del propio interesado, o bien para hacerlo sin recabar autorización judicial.

El TEDH, ahondando en la ausencia de normativa nacional propia sobre esta cuestión, considera que las normas reguladoras de la actuación policial no colman la exigencia de protección del derecho del art. 8.2 del Convenio. La sentencia analiza el valor de la jurisprudencia del Tribunal Constitucional como elemento integrador de las lagunas legales, considerando que el valor de la jurisprudencia constitucional es suficiente para colmar la ausencia de una disposición específica. En todo caso, analizando las resoluciones de nuestro Tribunal Constitucional constata que, en la mayor parte de las ocasiones, o bien se ha exigido el consentimiento del afectado, o bien se ha pedido la autorización judicial expresa para acceder a la limitación al derecho a la intimidad. Aplicando todo lo anterior al supuesto sometido a su consideración, el TEDH consideró conveniente estimar la alegación del recurrente sobre que no se había respetado la garantía debida a su derecho a la intimidad que había sido limitado.

El Tribunal Europeo también estudió las excepciones planteadas por el propio Tribunal Constitucional relativas a las situaciones de urgencia, como elementos justificantes de la actuación policial. Sobre estas situaciones de emergencia, el TEDH mantiene que, efectivamente, la urgencia prevista en una norma legal habilita para que se realice la actuación policial, incluso aunque ello suponga limitar un derecho fundamental previsto en el Convenio. Sin embargo, dado que el término emergencia resulta vago e impreciso hasta el punto de que incluso puede llegar a dar cierta cobertura a actuaciones arbitrarias o excesivas, el TEDH señaló que si existía un control judicial posterior sobre las medidas policiales urgentes, no deberían ser consideradas contrarias al contenido del CEDH.

La posibilidad de limitación del derecho a la intimidad de los ciudadanos, ante situaciones de urgencia está contemplada en el propio Convenio, y cabe llevarlo a cabo en situaciones que tratan de prevenir las acciones delictivas[322], lo que ocurre, por ejemplo, cuando se trata de evitar delitos en los que intervienen menores de edad.

Esta posible limitación de los derechos fundamentales de los ciudadanos ante situaciones en que la se trata de evitar un delito, es el origen de la doctrina de lo que se conoce como *«injerencia*

[322] . El TEDH usa la dicción literal del convenio "prevención de las infracciones penales" o la "protección de los derechos de los demás". Señala que "*las sevicias sexuales constituyen indudablemente un tipo odioso de delito que hace vulnerables a las víctimas" y que "los niños y otras personas vulnerables tienen derecho a la protección del Estado en forma de prevención eficaz que los resguarde de unas formas de injerencia tan graves en aspectos esenciales de su vida privada*".

necesaria en una sociedad democrática»[323]. En base a esta doctrina la limitación de un derecho esencial o fundamental es necesario, en una sociedad democrática, cuando se trata de alcanzar, mediante esa limitación, una finalidad legítima. Esta finalidad persigue satisfacer una *«necesidad social»,* y además ha de ser proporcionada en relación con el derecho limitado. Además, la medida finalmente adoptada ha de ser pertinente, suficiente y adecuada, para alcanzar este fin perseguido.

El TEDH terminó considerando que la actuación policial consistente en el examen de la carpeta de archivos de imagen, contenida en el ordenador personal del recurrente, podía estar amparada por tal urgencia, concretada en la necesidad de perseguir un delito de pornografía infantil, pero que el acceso al programa *emule* no estaba justificado. De hecho, el Tribunal estimó que había habido tiempo para haber recabado autorización judicial, sin que se justificara la emergencia, y que, además, esta premura también desaparecía en tanto que tener el ordenador intervenido hacía innecesaria cualquier medida urgente, y por ello concluyó apreciando que en el caso concreto existió una vulneración de los derechos contemplados en el convenio. El Tribunal sentenciador finalmente consideró que no se daban las razones para estimar la alta indemnización económica que solicitaba el demandante en su recurso.

En conclusión, cabe decir que el contenido de esta sentencia puso de manifiesto la necesidad de contar con habilitación legal para ejecutar diligencias de investigación, de manera urgente, por parte de los agentes de policía.

Este concreto aspecto se ha visto colmado con la regulación española actual, que en algunos casos admite, que por razones de urgencia se puedan adoptar medidas de investigación electrónica, que deben ser sometidas a una casi inmediata ratificación judicial. El concreto caso de la regulación de la diligencia de registro de un dispositivo de almacenamiento de información permite que se tome dicha información contenida en el dispositivo, ante situaciones urgentes, por parte de la policía, o bien por orden del Ministerio Fiscal, con la obligación de inmediato traslado al Juez para que ratifique o deje sin efecto la medida. En cambio, resulta interesante constatar que esta misma posibilidad no se da en la regulación sobre el registro remoto de equipos.

El examen de la sentencia pone al descubierto las carencias de la legislación anterior a la reforma sobre muchas de las cuestiones referentes a la garantía de los derechos fundamentales, e incluso acredita la insuficiente justificación jurisprudencial que existía respecto a dichas situaciones de urgencia, como circunstancias habilitantes para la limitación de estos derechos. Sin embargo, todo esto ha cambiado en la actualidad con la expresa admisión legal de la posibilidad de practicar

[323] Págs. 11 a 13 del texto de la Sentencia.

determinadas diligencias ante situaciones de emergencia. De manera que, deberá ser la jurisprudencia la que analice, caso a caso, si concurren tales situaciones excepcionales y urgentes.

La segunda sentencia que puede considerarse una influencia directa en el texto vigente de la LECrim fue la STC 145/2014, de 22 de septiembre[324], muy reseñada por la doctrina por su cambio de criterio con respecto a opiniones anteriores[325].

La sentencia analiza la práctica de una diligencia ordenada por el Juzgado de Instrucción número 5 de Zaragoza, que permitió unas escuchas de conversaciones realizadas en los calabozos de la Policía. El recurrente en amparo consideraba que no se habían respetado varios derechos de alcance constitucional, considerando vulnerados el derecho al secreto de las comunicaciones, relacionado con el derecho a no confesarse culpable y a no declarar contra sí mismo, como manifestaciones del derecho de defensa. También entendió que se había conculcado su derecho a la tutela judicial efectiva, en la modalidad del derecho al proceso con todas las garantías, porque fue condenado valorando unas pruebas, en concreto las escuchas, para las que no existía amparo legal alguno.

El Tribunal Constitucional en su sentencia va rechazando algunos de los motivos de amparo alegados por el recurrente, pero al analizar la alegación relativa a la ilegalidad de las escuchas practicadas en los calabozos, recuerda textualmente, que «*por mandato expreso de la Constitución, toda injerencia estatal en el ámbito de los derechos fundamentales y las libertades públicas, que incida directamente sobre su desarrollo (art. 81.1 CE), o limite o condicione su ejercicio (art. 53.1 CE), precisa, además, una habilitación legal*». Es decir, con esta manifiesta obviedad, se está recordando la insuficiencia del contenido del art 579.2 LECrim, que carece de las mínimas referencias que amparen según qué clase de acciones de investigación.

El hecho de que la diligencia practicada no contase con suficiente amparo legal llevó al Tribunal Constitucional a conceder el amparo al recurrente, pues, según sus palabras textuales *«la objeción reside, antes que en ello, en que abierta e inequívocamente la norma invocada no regula una intervención secreta de las comunicaciones directas en dependencias policiales entre detenidos. Disposición jurídica que es imprescindible, pues sólo con su fundamento puede existir imposición judicial de la medida en el caso concreto (STC 169/2001, de 16 de julio, FJ 6)».* Rechaza también la aplicación de normas penitenciarias al supuesto, tal como pedía el Ministerio Fiscal, porque estima que estas normas «*no rigen en un marco extrapenitenciario, ni están pensados para supuestos en los que no opera con toda su singularidad el régimen administrativo de especial sujeción propio del interno en un establecimiento de esa naturaleza»*

[324] STC 145/2014, de 22 de septiembre. Ponente: Don Fernando Valdés Dal-Ré.
[325] Vid. OTAMENDI ZOZAYA. Op. Cit. Pág. 98.

En conclusión, puede decirse de estas dos resoluciones que abundan, de manera específica, en el aspecto que hacía más inaplazable el cambio en la legislación. Una sentencia aborda la posibilidad de limitar derechos fundamentales en situaciones de urgencia, y la otra atiende a la necesidad de que se creara una habilitación legal expresa que permitiera realizar una determinada diligencia de investigación concreta. En suma, ambas demostraron, con ejemplos concretos, la necesidad de un cambio legislativo, que finalmente se produjo con la reforma operada por la Ley Orgánica 13/2015.

3. La diligencia de registro de dispositivos de almacenamiento masivo de datos.

La promulgación de la Ley Orgánica 13/2015, de 22 de septiembre, ha ampliado el catálogo de modalidades de investigación criminal que afectan a derechos de rango constitucional como el derecho a la intimidad, la propia imagen o el derecho al secreto de las comunicaciones[326]. La novedosa y revolucionaria cantidad de diligencias tecnológicas que se regulan en esta reforma supuso la incorporación a nuestro ordenamiento procesal penal de una nueva realidad jurídica que venía siendo reclamada por la doctrina, la de la investigación tecnológica de las conductas delictivas, lo que supuso colmar una evidente laguna del proceso penal español dada la clamorosa ausencia de cualquier tipo de norma que amparase el uso de la tecnología en la investigación, como se acaba de analizar.

Unos de los aspectos más relevantes y que convierten en especial a la nueva regulación, reside en la abundancia de las medidas y diligencias de investigación creadas; así como también a su originalidad y su esfuerzo de adaptación a los nuevos tiempos y a las nuevas necesidades sociales. Junto a eso, también hay que destacar el contraste que la nueva situación presenta con respecto a la inmediatamente anterior. Ni que decir tiene que el exiguo contenido del art. 579 LECrim, relativo a la intervención de comunicaciones electrónicas, sin mayores pormenores, contrasta con el alto grado de seguridad jurídica que la normativa vigente aporta. En la redacción actual se alcanza un mayor respeto y protección del contenido de los derechos constitucionales del art. 18, abundando en lo pormenorizado y casuístico que resulta el elenco de todas las medidas consignadas.

[326] Se debe destacar en todo caso que el interés de regular esta diligencia ya quedaba patente en el proyecto de Código Procesal Penal del año 2013, cuyos artículos 347 a 349 contenían una sucinta regulación de la materia. Sin embargo, que la regulación finalmente promulgada se caracteriza por ser mas extensa y prolija al trazar los límites y requisitos que ha de tener esta diligencia de investigación tecnológica. Puede consultarse el texto de dicho proyecto en el siguiente enlace del Ministerio de Justicia: http://www.mjusticia.gob.es/cs/Satellite/Portal/1292375190463?blobheader=application%2Fpdf&blobheadername1=Content-Disposition&blobheadername2=Medios&blobheadervalue1=attachment%3B+filename%3DCODIGO_PROCESAL_PENAL.pdf&blobheadervalue2=1288778173060. Pág. 170.

En esta parte del trabajo procede estudiar el contenido específico y concreto de las dos diligencias de investigación que se anunciaron en la introducción: la consistente en el acceso a dispositivos de almacenamiento masivo de información, que es la que se abordará en primer lugar, y la relativa al acceso remoto a equipos informáticos.

En el estudio de cada diligencia se irán analizando sus rasgos definidores, sus requisitos y sus características individuales, pero antes de eso, cabe hacer una reseña acerca de un aspecto que resulta común a ambas diligencias. Las dos diligencias de investigación que veremos comportan la concesión al Juez instructor, de la facultad de acceder y registrar datos albergados en un dispositivo que es apto para guardarlos. El dato que contienen estos artefactos se convierte en el nuevo paradigma de la investigación, transformándose en la fuente de prueba de la conducta delictiva que constituye la finalidad de dicha instrucción penal, porque de su estudio y análisis se puede extraer información que permita resolver aquellos aspectos esenciales del delito que no estén claros.

El dato, pues, se consagra como nuevo elemento primordial en la investigación penal, de importancia creciente, y de interés cada vez más habitual en las investigaciones. Además, en las dos diligencias que se analizan el objeto de la investigación son datos que se muestran completamente desligados de un proceso de comunicación, que era la forma más habitual de considerar el dato de esta naturaleza hasta ese momento.

Los puntos comunes entre ambas diligencias son tan evidentes como lo son también sus diferencias. En este sentido, la principal distinción entre las dos estriba en el modo en que se accede a los datos. El lugar puede ser idéntico en las dos diligencias, porque un dispositivo de almacenamiento puede ser un disco duro, pero también lo es un ordenador. Así en el caso de la primera diligencia, se llega a la información mediante la tenencia física del dispositivo, el cual, una vez aprehendido, es objeto de las operaciones de extracción de los datos que están contenidos directamente en su interior. Sin embargo, no se debe perder de vista que esta diligencia admite otra modalidad de acceso a los datos, completamente distinta, ya que permite entrar en dispositivos considerados “virtuales”, en los que se puede estar depositada información. En todo caso, cualquiera que sea su modalidad de realización, en esta diligencia, una vez registrados los datos contenidos en el dispositivo, procede su estudio y análisis, para relacionarlos con los hechos objeto de investigación y aportarlos a la instrucción.

En el caso de la segunda diligencia a analizar, la de registro remoto de equipos, lo que se utiliza es la tecnología para, mediante el uso de métodos informáticos, entrar de forma remota en el ordenador desde el que se realizan actos con trascendencia penal que se están investigando de manera que se hace innecesaria la presencia física ante el dispositivo. Esta diligencia permite el conocimiento, en directo, del empleo, creación, generación y obtención de los datos que resultan de

interés para la investigación emprendida, y todo ello desde el interior del ordenador. La finalidad de esta diligencia es similar a la de acceso a dispositivos de almacenamiento masivo de información, pues una vez registrado el artefacto, tras el acceso remoto al mismo se estudian y analizan los datos que se encuentren, para incorporar, los que procedan, a la instrucción penal.

En las dos clases de diligencias citadas se contempla, además, una modalidad particular de acceso a la información, nos referimos en concreto a cuando ésta se encuentra contenida en un sistema informático. El sistema informático, como concepto, puede ser entendido de varias formas, así puede concebirse como un complejo de formulaciones informáticas destinadas a cumplir una determinada actividad, pero también puede entenderse como el conjunto de máquinas interconectadas entre sí y que ofrecen servicios de gestión y control de la información. Bajo este amplio espectro es cómo debe ser entendido el concepto de dispositivo que nos ofrece la nueva legislación, lo que posibilita en nuestro Derecho, admita el acceso y registro de datos en dispositivos físicos, pero también en la nube. Pero hay variaciones con respecto a esto en las dos diligencias, pues en la primera no se realiza el acceso y el registro de modo remoto, y en el segundo si. En todo caso, lo importante para ambas diligencias es la obtención de datos. Éstos además exigen un examen posterior, a efectuar por un profesional cualificado. Es este el objeto perseguido por el análisis de los datos que serán objeto de un examen posterior realizado por un profesional cualificado. La finalidad perseguida con este análisis de los datos obtenidos es su interpretación y la aportación de esta al proceso, pues finalmente será esto lo que tendrá trascendencia penal llegado el caso.

La variedad de nuevas diligencias de investigación permite que se pueda, y se deba, diferenciar entre los distintos tipos de datos. En este sentido, puede decirse que hay datos derivados de un proceso de comunicación, y otros datos que no.

En el caso de las dos diligencias analizadas, los datos no deben formar parte de un proceso de comunicación, pues de formar parte de ese proceso comunicativo habría que acudir a las diligencias específicas que contiene la LECrim para el acceso a los elementos de una comunicación telemática definidos como «*los datos electrónicos de tráfico o asociados al proceso de comunicación, así como los que se produzcan con independencia del establecimiento o no de una concreta comunicación, en los que el partícipe sea el sujeto investigado, ya sea como emisor o como receptor, y podrá afectar a los terminales o los medios de comunicación de los que el investigados*

sea titular o usuario»[327]. En cambio, no existe inconveniente en que los datos que se recaben sean relativos a una comunicación ya finalizada.

En suma, de lo que se trata es de encontrar datos que hayan quedado dentro de un dispositivo, y a los que se debe acceder para poder analizarlos y estudiarlos para continuar con el avance de la investigación en curso [328].

El segundo de los aspectos común a las dos diligencias de investigación, es que ambas parten de la existencia de un aparato o un dispositivo en cuyo seno se encuentra alojada información de interés para la investigación criminal. Sobre esta característica común, la diferencia entre ellas estriba en que, mientras en la diligencia de acceso al dispositivo de almacenamiento masivo, se practica sobre un dispositivo encontrado de forma efectiva y física (incluyendo aquí la fórmula virtual de deposito de información realizada en la nube), no sucede igual en la que consiste en el acceso remoto. En esta segunda medida se parte de que hay un conocimiento cierto, o al menos indicios suficientes, de que el ordenador se emplea para la comisión de un delito, pero, para recoger los datos que lo acrediten, se emplean los medios tecnológicos que permiten literalmente bucear en el interior del dispositivo en busca de la información de interés para la investigación, sin necesidad de estar físicamente delante del ordenador[329].

3.1. Antecedentes jurisprudenciales sobre el acceso a la información contenida en dispositivos electrónicos.

El uso de dispositivos capaces de almacenar datos diversos en su interior (fotografías, archivos de audio, texto o mensajes recibidos y enviados) es una realidad ya asentada en nuestra vida cotidiana desde hace años. A nadie le resulta extraño ya el uso de lápices de memoria, discos duros externos, y toda clase de aparatos cuya finalidad es recoger, conservar, proteger, y hacer disponible nuestra información personal, en cualquier momento y en cualquier lugar. Este uso ordinario y extendido

[327] El Art. 588 ter apartado b, párrafo 2 LECrim nos ofrece esta definición de proceso de comunicación. Es por ello evidente que teniendo en cuenta esta definición, deberemos aplicarla como proceso reflexivo previo a la petición de cualquier diligencia de investigación, o bien a la previa fase de concesión de la misma realizada por el Juez Instructor. Pues si del resultado de ese proceso de reflexión resulta viable que la diligencia que se solicita pueda comportar el acceso a las comunicaciones sería muy aconsejable que esto se recogiera tanto en el oficio de solicitud como, posteriormente en el auto que resuelve sobre esta petición. Entiendo que partiendo de la aplicación del principio de especialidad, y existiendo una previsión legal que contempla el acceso a este tipo de derecho esencial, debe recogerse así tanto a la hora de solicitarse la diligencia, como a la hora de motivar la concesión o denegación de la misma.

[328] Vid. ORTIZ PRADILLO, Juan Carlos. *Problemas procesales de la ciberdelincuencia*. Colex. Madrid. 2013. Pág. 176.

[329] Este aspecto de la norma es muy novedoso, porque realmente, con independencia de que el estado de la tecnología actual permita o no realizar dicho tipo de acceso, la realidad normativa lo permitiría.

también alcanza a la actividad delictiva, en la que los datos que sirven para la ideación, preparación y ejecución de la comisión de un delito, o los que acreditan su realización efectiva, quedan guardados, o a disposición de los partícipes de la misma dentro de un dispositivo.

Los datos que pueden acreditar, de forma directa o indirecta, un hecho delictivo pueden ser de muchos tipos. Por ejemplo, el acceso a internet efectuado a una hora determinada, el acceso a una concreta web, la determinación de una dirección IP, la localización GPS que se puede extraer de un dispositivo, etc. Todos estos datos, debidamente analizados, pueden permitir, con el establecimiento de las debidas relaciones lógicas, que se averigüen hechos delictivos.

El estudio de los datos albergados en dispositivos electrónicos ha sido tratado por los tribunales de Justicia antes de la reforma procesal de 2015. En dichas resoluciones judiciales, pioneras en nuestro país en el análisis de estas cuestiones, lo primero que se planteaba era determinar qué derecho fundamental se afectaba cuando se accedía a la información que se encontraba en un dispositivo electrónico, y también se planteaban cuál debía ser el mecanismo que amparase dicho acceso[330].

El Tribunal Supremo ha ido asociando el uso de ordenadores, por el contenido de los datos que estos albergan, con la idea de uso de un instrumento que guarda una relación directa con el derecho a la intimidad[331]. Se descarta, en esas sentencias, la afectación de algún otro derecho fundamental distinto a éste[332].

Precisamente, el constante cuestionamiento de cuáles son los derechos constitucionales afectados en situaciones como éstas, ha sido uno de los aspectos que ha influido en la evolución de la jurisprudencia hacia el reconocimiento del derecho al propio entorno virtual, tal y como ya vimos

[330] STS 187/2015, de 14 de Abril. Ponente: Don Francisco Monterde Ferrer. En la sentencia se hace un análisis acerca del modo de acceder a un pendrive, sobre todo en los fundamentos de derecho sexto y séptimo. Se establece en primer lugar que el derecho afectado cuando se accede al mismo no es el derecho al secreto de las comunicaciones, sino el derecho a la intimidad. En el caso la orden de entrega del dispositivo se acordó mediante una providencia, estableciendo en este caso el TS que aunque la correcta resolución que permita la entrega del pen drive debió ser un auto, ello alcanza sólo el matiz de irregularidad procesal sin trascendencia en los derechos del afectado. En todo caso se aprecia que la resolución de acceso, análisis y estudio de los datos contenidos en el pen drive adoptó la forma de auto. También señala la importancia de la cadena de custodia de la información contenida en el dispositivo, la innecesaria presencia del Letrado de la Administración de Justicia en el volcado de los datos (estableciendo que lo esencial es que se certifique que los datos aportados a las actuaciones se corresponden con los que existían en el dispositivo), y también establece en tercer lugar, como aspecto importante, la innecesaria presencia del investigado en la diligencia del volcado de los datos.

[331] STS 358/2007, de 30 de abril. Ponente: Don Miguel Colmenero Menéndez de Luarca. En la sentencia, el TS aborda en base al tipo penal de la revelación de secretos, el acceso a los datos contenidos en un ordenador que era de titularidad pública. Entendido a sensu contrario su contenido, el Alto Tribunal señala que es ordenador es un lugar idóneo para poder alojar esta clase de datos íntimos.

[332] Así, y sobre si pudiera quedar afectado el derecho al secreto de las comunicaciones, se excluye esta posibilidad. Se considera que en lo que se refiere a las comunicaciones, en el ordenador sólo quedaría el rastro de procesos de comunicación que ya se habrían agotado. Así por ejemplo podrá quedar el rastro de datos dejado tras una conversación por Skype o por FaceTime, pero ésta ya estaría conclusa, o bien podría quedar el correo ya abierto. Es por eso por lo que el derecho que estaría afectado en estos casos sería el derecho a la intimidad, en cuanto que tales datos están protegidos por el mismo, pero no el derecho al secreto de las comunicaciones, en tanto que éstas ya están terminadas. En el caso de que lo que fuera encontrado fuesen imágenes o fotografías, además de la intimidad ya aludida, podría suscitarse la posibilidad de que se viera afectado el derecho a la propia imagen.

en otras partes de este trabajo. La protección de las evidencias digitales que un individuo deja tras de sí, por el empleo de la tecnología, elevándola a la categoría de un derecho con autonomía propia, supone la decantación de un proceso que ha pasado de considerar por separado todos los derechos concurrentes, a tomar en consideración la actividad digital integra en su conjunto, esto es, como un solo acto del individuo en el que se superponen varios derechos fundamentales que concurren simultáneamente. De hecho, resulta demasiado reducido el planteamiento de considerar que el acto de usar un ordenador, y las diferentes aplicaciones que tiene, solo afecta a un sólo derecho fundamental, cuando la realidad es que están afectados varios a la vez.

Los tribunales no sólo han sido los creadores del concepto de derecho al entorno virtual, en su análisis de la actividad informática, sino que también han ido desarrollando determinados conceptos relacionados con esta clase de actividades, algunos de los cuales, en la actualidad, figuran en el texto regulador de las diligencias de este estudio.

Al respecto, podemos poner dos ejemplos de cómo se han analizado las actividades informáticas para traducirlas a la problemática jurídica que en cada caso se planteaba.

En un primer momento, la posición de la doctrina jurisprudencial sobre el registro de dispositivos informáticos consistía en asimilarlos, desde su conceptuación jurídica, a la diligencia de toma y exhibición de libros y de papeles, que sí estaba expresamente contenida en la LECrim[333]. Esta asimilación posibilitaba que el auto de entrada y registro en domicilio particular habilitase para poder incautar los soportes informáticos encontrados en ella[334], y también acceder a su contenido. Posteriormente esta doctrina se vio reformada hacia la posición justamente contraria, y ahora se

[333] Art. 575 LEcrim.

[334] La STS 256/2008, de 14 de mayo. Ponente: Don Perfecto Andrés Ibáñez, que a su vez se pronuncia sobre la SAP de Madrid 154/2007, de 9 de abril. Ponente: Doña Araceli Perdices López, confirmándola. La resolución de la Audiencia Provincial estableció en relación al auto dictado por el Juzgado de Instrucción «*acordando la entrada y registro en el domicilio del procesado, en el que se menciona el delito que se estaba investigando y se autorizaba la intervención "de los documentos, material informático, agendas o manuscritos, u otros efectos de similares características (soportes informáticos) que pudieran contener datos directamente relacionados con los hechos investigados", de forma tal que los ordenadores con todo su contenido quedaban incluidos dentro de esa autorización que posibilitaba no solo su comiso sino por ende el análisis de su contenido,* (subrayado es nuestro), *debiendo considerarse la providencia de fecha 23 de septiembre de 2005 que autorizaba el análisis de la información contenida en los dos ordenadores, como una corroboración de los anterior, sin que la circunstancia de que durante el volcado de la información no estuviera presente un Secretario Judicial ni el imputado o su representante invalide la prueba».* Otro ejemplo similar podemos encontrarlo en la SAP de Madrid 1235/2002, de 27 de junio. Ponente: Don José Antonio Ramos Gancedo. Esta resolución pone de manifiesto ante la necesidad de leer un mensaje contenido en un teléfono móvil que *«la apertura de una agenda del detenido, su examen y la lectura de los papeles que se encontraban en su interior (equivalente a la "apertura" del teléfono móvil para examinar y leer los mensajes ya recibidos) supone una intromisión en la esfera privada de la persona a la que tales efectos pertenecen, esto es, en el ámbito protegido por el derecho a la intimidad. Pero, sentado ésto -y siempre abstracción hecha del Auto judicial habilitante que en el caso que examinamos legitimaba la actuación policial-, se trataría de una diligencia practicada por la policía judicial en el curso de la investigación de un grave delito tras la detención del propietario del móvil, y orientada a la averiguación del mismo y a la recogida de instrumentos, efectos y pruebas de aquél, además de allegar información respecto a otros eventuales partícipes en la actividad delictiva investigada. Por tanto, concurriría un fin constitucionalmente legítimo».*

necesita permiso para entrar en el domicilio y aunque se confisque un aparato, también se necesita habilitación especial para poder acceder a su contenido.

El segundo ejemplo lo encontramos en la alocución "repositorio de datos", que en la actualidad esta recogida en la regulación de la diligencia que regula el acceso a dispositivos de almacenamiento masivo de información[335].

En algún análisis jurisprudencial se han destacado, como notas esenciales de estos repositorios, de un lado, el hecho de su carácter externo al ordenador, y de otro lado que su finalidad ha de ser permitir el acceso de los particulares a los datos que contienen. El uso que se les da a tales repositorios es tanto alojar información, como permitir que los sujetos puedan servirse del contenido de los mismos[336]. El estudio realizado por la jurisprudencia también se ha adentrado en su posible carácter público, esto es de acceso libre para todas las personas, pero con la posibilidad de convertirlo en un instrumento de uso privado restringiendo el acceso a personas habilitadas para acceder a la información contenida en el repositorio.

En este sentido, no se debe perder de vista que es un tipo de servicio que permite crear un lugar en el que se deposita información por parte de una persona a la que más tarde se puede volver a acceder, y al mismo tiempo, también permite que otro sujeto también pueda acceder para recabar los datos depositados allí, o modificar los existentes.

Lo mismo que sucedía en el ejemplo anterior respecto de los dispositivos de almacenamiento masivo de información, en el caso de los repositorios de datos también la jurisprudencia ha intentado analizar inicialmente este tipo de servicio partiendo de su ubicación dentro del ámbito de los derechos fundamentales afectados, de su utilidad, pero siempre desde la óptica de qué derechos son los que pudieran verse afectados.

En suma, lo que cabe destacar en este momento es que la jurisprudencia, anterior a la entrada en vigor de la reforma de la LECrim, no ha sido ajena a la existencia de dispositivos de

---

[335] Ver el contenido del art. 588 sexies b. LECrim.

[336] STS 789/2014, de 2 de diciembre. Ponente: Don Juan Ramón Verdugo y Gómez de la Torre. La sentencia realiza una definición de mecanismos de acceso por parte de los investigados a diferentes sitios alojados en internet desde el que realizan la actividad que estaba siendo objeto de investigación (en el caso examinado por la sentencia estamos ante un supuesto de adoctrinamiento yihadista). Así dice la sentencia que «*Los repositorios de acceso público están concebidos como espacios de almacenamiento de contenidos digitales de acceso público*". Sigue diciendo a continuación que: «*Frente a otros repositorios existentes en internet, archive.org ofrece las características del anonimato (pues sus usuarios sólo tienen que crear una cuenta utilizando una dirección de correo electrónico y una contraseña a su elección, sin aportar más datos personales, para iniciar el proceso de subida de archivos desde su ordenador), gratuidad (puesto que el alojamiento de contenidos no supone coste alguno para quienes los suban), difusión (ya que los contenidos alojados pueden ser descargados por cualquier usuario a través del enlace de descarga que genera el sistema), permanencia (pues tales contenidos sólo pueden ser editados y borrados por el usuario que los ha subido), capacidad ilimitada (pues no existe tope en cuanto a la cantidad y tamaño de los archivos subidos) y multiformato (al contar el sistema con potentes herramientas de conversión de archivos a diferentes formatos)»*.

almacenamiento de datos. De hecho, se puede decir que, la actual normativa no es más que el fruto de la evolución jurisprudencial referente al acceso y el registro de dispositivos que contienen información digital. Esta evolución ha sido lenta y paulatina, y se ha ido desarrollando desde una posición muy apegada al contenido de cada derecho fundamental afectado por la diligencia de investigación analizada, a otra postura mucho más abstracta y aglutinadora de todos los derechos que están implicados. Pero también se han ido perfilando y asimilando distintos modos de ejecutar o de llevar a cabo los actos concretos de investigación, asociándolos al contenido de otras diligencias de investigación existentes en ese momento.

Por otro lado, también se puede constatar que la jurisprudencia ha analizado el empleo de nuevos medios tecnológicos (como, por ejemplo, los repositorios de datos) con trascendencia en la investigación penal.

En este segundo grupo de casos, ha sido la falta de legislación sobre los medios de investigación tecnológica, unido a la ineludible necesidad de dar respuesta a cada caso, la que ha dado como resultado una jurisprudencia calificada por la doctrina como carente de uniformidad sobre estas materias[337]. Pero, a pesar de ello, es necesario destacar la indudable influencia que la nueva regulación ha recibido de la jurisprudencia anterior a la reforma, pues de hecho, muchos de sus principios parten de ella, como ya hemos reseñado en algún otro apartado, siendo esta influencia reconocida por la propia Exposición de Motivos de la Ley Orgánica 13/2015.

3.2. Requisitos y presupuestos para su adopción.

La recepción de la diligencia de acceso y registro de dispositivos electrónicos dentro de la LECrim se hizo *«respondiendo a la obligación derivada del el art. 19.2*» del Convenio de Budapest sobre ciberdelincuencia, como ha señalado expresamente la doctrina[338]. En concreto, su regulación específica está contenida en el Capítulo VIII del Título VIII de la LECrim, bajo la denominación de diligencia de registro de dispositivos de almacenamiento masivo de información.

[337] MARCHENA GÓMEZ, GONZÁLEZ CUÉLLAR SERRANO. Op. Cit. Pág. 370.

[338] Cfr. DELGADO MARTÍN, Joaquin. «Investigación del entorno virtual…». Op. Cit, Pág. 10. El autor sitúa en el citado artículo origen de « *los nuevos arts. 588 sexies a.1 y 588 sexies b LECrim. se refieren expresamente al «acceso a repositorios telemáticos de datos», y lo somete al mismo régimen jurídico que el registro de dispositivos de almacenamiento masivo que se ha examinado anteriormente: necesita autorización judicial, salvo casos de urgencia de la intervención policial*».

El Capitulo se distribuye en tres artículos; desde el art. 588 sexies, apartado a), hasta el art. 588 sexies apartado c) LECrim[339].

Para conocer en profundidad esta diligencia de investigación es necesario efectuar un recorrido por su génesis y elaboración, en tanto que estos aspectos determinan la redacción de su tenor literal, a los efectos de poder conocer su casuística, sus presupuestos y los requisitos necesarios para su adopción.

Lo primero que destaca dentro del contenido de sus preceptos es la importante flexibilidad de la que es dotada esta diligencia por el legislador a la hora de poder ser aplicada a un caso concreto. Es una diligencia que puede servir para investigar cualquier hecho con trascendencia penal, sin distinción alguna. A diferencia de otras diligencias de investigación, y más específicamente, con respecto a la de intervención remota de equipos informáticos, la diligencia de acceso a dispositivos de almacenamiento masivo de información, puede acordarse para realizar la investigación de cualquier modalidad delictiva, sin que importe su gravedad. Este extremo se deduce por remisión a las normas comunes contenidas en el art. 588 bis LECrim[340], que no exigen su aplicación para determinados tipos penales. Este aspecto generalista la diferencia del carácter mucho más restringido que se le debe atribuir a la diligencia de acceso remoto a equipos informáticos, más dirigida a la investigación de delitos muy concretos y mucho más graves.

La ausencia de limitación en los tipos penales que se pueden investigar mediante el empleo de esta diligencia de registro de dispositivos de almacenamiento masivo de información, permite concluir con que la información contenida en dispositivos de esta naturaleza puede ser usada para investigar cualquier clase de actuación penal, sea del tipo que sea, con independencia de su gravedad o alarma social que la misma genere (y que pueden ir desde una simple amenaza hasta un delito de terrorismo, o desde unas lesiones simples hasta un asesinato). Esta posibilidad tiene sentido, en

[339] Es este último precepto el que concentra, de forma prolija, algunas de las cuestiones más polémicas que se derivan de la regulación de esta diligencia de investigación.

[340] Auto AP de Barcelona 214/2017, de 1 de marzo. Ponente: Doña Elena Guindulaín Oliveiras. En la resolución se indica sobre el particular: «*Frente al ejemplo de otras modalidades de tecnovigilancia, en las que sí se incluyen listas de delitos que pueden dar lugar a su empleo, el art. 588 sexies a no recoge infracción criminal alguna; por lo que habremos de acudir a los criterios valorativos comunes antes referidos; sin perjuicio de partir del incontestable estándar del concepto de delito grave que vendría representado por el delito castigado con penas de prisión que en su máxima expresión alcance al menos los tres años de prisión. No es que defendamos, y más en un contexto de menor intensidad de la injerencia, que este concepto ad hoc de delito grave sea un límite infranqueable; pero el distanciamiento de este referente hará precisa una más justificada ponderación de todos los factores que condicionan la superación del juicio de proporcionalidad*». Ciertamente el contenido del auto parece referir que en todo caso se necesita que estemos ante delitos penados con al menos tres años de prisión, lo cual sólo resulta exigible en las diligencias que tengan relación con la intervención de las comunicaciones como se exige del tenor del art. 588 ter a, puesto en relación con el art. 579.1, ambos de la LEcrim.

tanto que, cada vez con mayor frecuencia se emplea la tecnología para la comisión de cualquier clase de delito[341]

Sin embargo, en todo caso, es el juez instructor habrá de valorar el contexto y las circunstancias del hecho cometido, procurando el respeto de los principios generales aplicables a toda medida que limite los derechos constitucionales del afectado. En este sentido, aunque todos los principios del art. 588 bis a LECrim son fundamentales, debe vigilarse por el juzgador, en especial, la aplicación del principio de proporcionalidad, pues es un elemento discriminador fundamental para realizar la necesaria ponderación entre lo que ha pasado y la diligencia restrictiva de derechos que se le pide.

El segundo rasgo a reseñar sobre el contenido de los arts. 588 sexies apartados a y b LECrim, es que en estos preceptos se enumeran los dispositivos a los que puede afectar la practica de esta diligencia de investigación. En todo caso, y pese a la variedad, de dispositivos enumerados en el tenor legal, todos comparten el hecho de que «*la información que se contiene en estos dispositivos puede tener distinto origen: datos técnicos del sistema respecto a su funcionamiento, dispositivos conectados, comunicaciones establecidas, documentos de texto, imágenes, sonido, etc»*[342]. Por tanto, se trata de una enorme variedad de artefactos que abarca desde ordenadores, a instrumentos de comunicación telefónica o telemática, dispositivos de almacenamiento masivo de información digital y repositorios telemáticos de datos[343].

Aunque el legislador enuncia determinados aparatos, no hay razón para entender que estamos ante un *numerus clausus* o lista cerrada de dispositivos. La evolución que experimenta la tecnología demuestra lo obsoleto que puede quedar un artefacto en cuestión de meses y, ante este hecho, es aconsejable, que pueda extenderse la practica de esta diligencia a otros artefactos distintos a los enumerados expresamente por la Ley.

En todo caso más que el nombre que se le de al dispositivo, lo esencial es la función que tiene que cumplir el mismo[344]. Por consiguiente, mientras el dispositivo sirva para la acumulación de datos

---

[341] Un caso que acontece con mucha frecuencia suele ser el de estafas cometidas mediante el empleo de redes sociales. Suele tratarse de la venta de enseres electrónicos como teléfonos o videoconsolas usando aplicaciones creadas para ello, y que suele ser de cantidades inferiores a cuatrocientos euros, y en ellos suele ser común la práctica de diligencias de registro de determinados dispositivos en los que quede constancia de la conversación, la transferencia, etc.

[342] Cfr. RICHARD GONZÁLEZ, Manuel. «Conductas susceptibles de ser intervenidas por medidas de investigación electrónica. Presupuestos para su autorización». *Diario La Ley*, Nº 8808, 21 de Julio de 2016, LA LEY 5735/2016 I. Pág. 10.

[343] Algún autor considera que esta mención hace extensible la aplicación de la medida a los datos alojados en la nube; así Vid. OTAMENDI ZOZAYA, Fermín. «La ansiada regulación de las llamadas medidas de investigación tecnológica», en OTAMENDI ZOZAYA, Fermín. *Las últimas reformas de la ley de enjuiciamiento criminal. Una visión práctica tras un año de vigencia*. Op.Cit. Pág. 139. https://app.vlex.com/#vid/ansiada-regulacion-llamadas-medidas-685885029.

[344] En todo caso la doctrina considera que la enumeración efectuada no agota el número de artefactos o de dispositivos a los que puede afectar, sino que le será aplicable a cualquier dispositivo que sirva para alojar información o datos que sean de interés para la investigación, incluso aunque dichos datos los contenga de manera temporal (GPS, router, o

(por ejemplo un router[345], un ordenador, una tablet, un GPS[346], o cualquier otro similar), puede entenderse que, pese a que no esté dentro de la enumeración efectuada por la norma, es posible practicar la diligencia sobre ellos.

La enorme amplitud de dispositivos que ofrece el mercado para alojar datos permite que podamos acogernos a una dicotomía simple al referirnos a ellos, o a la hora de clasificarlos. Los dispositivos pueden dividirse entre instrumentos que presentan una realidad física y aquellos otros que son dispositivos virtuales. Pero, en todo caso, ambos tipos de instrumentos ofrecen, con carácter común, la posibilidad de alojar en su interior toda clase de datos. Este hecho los convierte en un medio apto para ser registrado mediante la diligencia analizada[347].

El alojamiento de los datos puede hacerse tanto físicamente (por ejemplo, cuando guardamos un documento o una fotografía en un pen drive), como empleando otro artefacto o instrumento que sirve de vía de acceso al depósito de datos. En este último caso estamos ante la *nube,* que constituye un medido apto para albergar datos, pero que no está presente físicamente en ningún lugar, sino que se emplea un ordenador o cualquier otro dispositivo que permita acceder a ella y operar con los datos allí almacenados. Cuando se hace uso de los servicios *cloud* lo que se hace es aprovechar cualquier dispositivo con conexión a internet y es mediante éste como se accede al servicio de alojamiento en la nube. Pero caben otros casos de uso virtual, como por ejemplo el empleo de una red de servidores de una empresa (intranet). En los dos casos los datos no están en el ordenador del usuario, pero se emplea éste para poder acceder al lugar digital en el que se encuentra almacenada la información.

La enumeración de los dispositivos es seguida por una descripción del contexto espacial en el que aparecen estos dispositivos. Es decir, se refiere a la situación y circunstancias de lugar en la que estos instrumentos son encontrados.

---

cualquiera de los mecanismos previstos en el art. 197.2 bis del CP como susceptibles de ser empleados en la comisión de un delito de revelación de secretos en la modalidad de datos informáticos, etc.). Así, puede consultarse Vid. MARTÍN MARTÍN DE LA ESCALERA, A, M. «El registro de almacenamiento masivo de la información. Ponencias de Formación organizadas por la Fiscalía General del Estado». Jornadas de 27 de abril de 2016 tituladas "La interceptación de las Comunicaciones telefónicas y telemáticas". Texto contenido en el enlace web: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20Martín%20Martín%20de%20la%20Escalera,%20Ana%20Mª.pdf?idFile=bf66c357-e4d4-4701-8a4d-83d6c103ebe5. Pág. 5.

[345] SAP de Bilbao 90097/2017, de 12 de abril. Ponente: Doña Elisa Pisonero del Pozo Riesgo. En la sentencia se realiza una pericial sobre un router a los efectos de extracción de datos para la causa.

[346] STS 249/2008, de 20 de mayo. Ponente: Don Manuel Marchena Gómez. La sentencia estima que la autorización judicial habilita para el análisis o la intervención del GPS instalado en este caso en una embarcación.

[347] La Circular de la Fiscalía General del Estado 5/2019, de 6 de marzo, contiene en sus págs. 9 a 11 una definición de dispositivo, así como una distinción entre soporte de almacenamiento y dispositivo de almacenamiento. En todo caso la Circular sostiene también la amplitud de la categoría admitiendo desde los electrodomésticos que actualmente admiten la conservación de datos hasta los dispositivos que lo hacen de modo telemático.

La norma diferencia según que el dispositivo se encuentre dentro de un domicilio al que se ha accedido previamente o que, por el contrario, sean hallados fuera de un inmueble que sirva como morada. La distinción termina siendo tratada, desde la óptica de la limitación-protección del derecho, del mismo modo. Por eso es una distinción un tanto innecesaria.

La norma parte de dos supuestos: el hallazgo de alguno de estos dispositivos de almacenamiento masivo durante el transcurso de un registro domiciliario (art. 588 sexies a) LECrim), y la ubicación del dispositivo fuera de dicho domicilio (art. 588 sexies b) LECrim). A los efectos de la definición de domicilio deben aplicarse las reglas legales y la jurisprudencia que deslindan el concepto de lo que es un domicilio y lo que no lo es[348].

En todo caso, y con independencia del lugar en que el dispositivo sea encontrado, esto no influye en la manera de acceder y registrar la información que se encuentre el interior del artefacto, cuyas exigencias y requisitos son comunes en los dos supuestos.

En concreto, estos artículos lo que exigen es una expresa autorización judicial para poder realizar el acceso a los datos que hay dentro del dispositivo encontrado. En este sentido, hay que destacar que lo que se requiere en la legislación para poder practicar esta diligencia no es una autorización simple, es decir no se trata de un mero dar permiso, sino que ha de ser una auténtica autorización jurisdiccional, en la que se contenga la decisión motivada de permitir de forma expresa la realización de la diligencia de registro del dispositivo.

De hecho, el art. 588 sexies a) LEcrim alude a la *«necesidad de motivación individualizada»* de las razones para acceder registrar y analizar los datos que están en el interior de un dispositivo localizado durante un registro. Aparece aquí, como ocurre en las demás diligencias, y como se

[348] Sin ánimo de exhaustividad, debe recordarse que el concepto de domicilio ha sido fijado por la jurisprudencia del Tribunal Constitucional. La STC (Pleno) 10/2002, de 17 de enero, recuerda dicha doctrina estableciendo que: «*La Constitución no ofrece una definición expresa del domicilio como objeto de protección del art. 18.2 CE. Sin embargo, este Tribunal ha ido perfilando una noción de domicilio de la persona física cuyo rasgo esencial reside en constituir un ámbito espacial apto para un destino específico, el desarrollo de la vida privada. Este rasgo, que ha sido señalado de forma expresa en Sentencias recientes (SSTC 94/1999, de 31 de mayo, F. 4; 283/2000, de 27 de noviembre [RTC 2000, 283] , F. 2), se encuentra asimismo comprendido en las declaraciones generales efectuadas por este Tribunal sobre la conexión entre el derecho a la inviolabilidad domiciliaria y el derecho a la intimidad personal y familiar, así como en la delimitación negativa que hemos realizado de las características del espacio que ha de considerarse domicilio y de la individualización de espacios que no pueden calificarse de tal a efectos constitucionales.*
Con carácter general, como acabamos de recordar, hemos declarado que «el domicilio inviolable es un espacio en el cual el individuo vive sin estar sujeto necesariamente a los usos y convenciones sociales y ejerce su libertad más íntima. Por ello, a través de este derecho no sólo es objeto de protección el espacio físico en sí mismo considerado, sino lo que en él hay de emanación de la persona y de esfera privada de ella» (SSTC 22/1984, de 17 de febrero, F. 5; 137/1985, de 17 de octubre [RTC 1985, 137] , F. 2; 69/1999, de 26 de abril [RTC 1999, 69] , F. 2; 94/1999, de 31 de mayo, F. 5; 119/2001, de 24 de mayo, FF. 5 y 6)». Se trata de un concepto que ha generado numerosas polémicas sobre cuestiones muy diversas, que van desde qué debe considerarse domicilio (por ejemplo, las embarcaciones o los garajes - objeto de las STS 513/2014, de 24 de junio. Pte: Juan Ramón Berdugo Gómez de la Torre, o STS 468/2015, de 16 de julio. Pte: Don Andrés Palomo del Arco-) hasta si las personas jurídicas lo tienen o no.

desprende de la aplicación de los principios rectores, la exigencia y la necesidad de motivación especifica, que se erige como un auténtico paradigma de la nueva regulación.

La diligencia de registro de dispositivos de almacenamiento masivo de información, como las demás diligencias de investigación electrónica, exigen para ser aplicadas un verdadero ejercicio de explicación y motivación de las razones por las que se aconseja la intromisión en el contenido que alojan. No cabe en ningún caso que se lleve a cabo un acceso automático al contenido de estos dispositivos y que el mismo se lleve a cabo carente de cualquier razonamiento sobre su necesidad. Por el contrario, atendida la finalidad que se perseguía con la reforma procesal de 2015, que no era otra que la de aumentar las garantías procesales, y en este caso, especialmente, a los derechos del art 18 CE, se consigue dicha protección atribuyendo un control jurisdiccional a estas acciones, que se ejerce mediante el ejercicio de motivación. Por otro lado, cuando el instrumento que contiene la información se localice fuera de un lugar que pueda ser considerado domicilio, la respuesta legal es idéntica[349].

La autorización judicial es necesaria siempre para efectuar el acceso a la información que contengan los dispositivos encontrados, con independencia del lugar en que esto suceda[350]. En todo caso esta distinción, que estimo innecesaria, se puede comprender si lo que dispone la norma en la actualidad se compara con las situaciones jurídicas anteriores a la reforma de la LECrim de 2015, en las que la autorización para entrar en domicilio, se hacía extensible al acceso a dispositivos encontrados en su interior. Esta situación es la que el legislador pretendió erradicar con la nueva regulación. Por esa razón, la autorización judicial tiene que ser específica y distinta de la que permitió acceder al domicilio. De hecho, con la nueva regulación ambas situaciones quedan completamente separadas. Y así, se necesitarán dos autorizaciones para llevar a cabo esta diligencia: una para el acceso al domicilio (que puede comprender la facultad de incautar los instrumentos encontrados en el interior de éste y que pudieran ser útiles a la investigación), y otra para acceder al contenido de los dispositivos encontrados[351].

---

[349] Es por esto por lo que alguna doctrina considera «*innecesaria»* la distinción realizada. Cfr. OTAMENDI ZOZAYA, Fermín. Op. Cit. Pág. 140.

[350] En palabras del Informe del Consejo Fiscal al Anteproyecto de Ley Orgánica de modificación de la Ley de Enjuiciamiento Criminal para la agilización de la Justicia penal, el fortalecimiento de las garantías procesales y las medidas de investigación tecnológica (Pág. 114). «*La previsión …. es pertinente para poner fin a la práctica judicial que entendía que la autorización jurisdiccional para la entrada y registro en un inmueble conlleva la habilitación implícita para acceder a los dispositivos de almacenamiento masivo que puedan allí encontrarse, desconociendo como se ha expuesto por la doctrina, la sustantividad propia del derecho a la intimidad y eventualmente al secreto de las comunicaciones, derechos que no pueden quedar artificialmente absorbidos en el ámbito de la protección constitucional del domicilio».*

[351] Ciertamente con esta disposición contenida en la LECrim, se pone fin a las dudas que podría suscitarse caso por caso ante la necesidad de recabar autorización judicial independiente a la que habilita para la entrada y registro en domicilio. La STS 691/2009, de 5 de junio. Ponente: Don Adolfo Prego de Oliver y Tolivar; contiene en su fundamento de derecho segundo, punto 3 la siguiente manifestación: «*Y en el caso presente el CD intervenido en la diligencia de*

El fundamento de la distinción reside en que se limitan dos derechos distintos: la inviolabilidad del domicilio -art. 18.2 CE- y el derecho a la intimidad, o bien, de un modo más preciso, dada la multiplicidad de posibles derechos afectados al acceder al contenido del dispositivo de almacenamiento masivo de la información, el *derecho al propio entorno virtual*, si así se prefiere. Esto exige un razonamiento judicial separado, independiente y autónomo o como dice el precepto *"motivación individualizada"*.

La jurisprudencia ha tenido que pronunciarse sobre situaciones en las que debidamente autorizada una entrada y registro en domicilio, una vez en el interior del inmueble, se ha accedido al contenido de algún dispositivo encontrado durante su practica[352]. Se generaban controversias acerca tanto del tipo de derecho afectado, como de la necesidad del consentimiento del afectado, y si era necesaria

---

entrada y registro, legítimamente practicada, y que conforme a la inscripción del soporte contenía información oficial, no personal, el acceso a su contenido no implica injerencia en datos personales o íntimos, sino que bien cabría calificarlo como documento en soporte diferente al papel y encuadrable en el concepto de que de tal da el art. 26 del CP, y la lectura de su contenido al no afectar ni a la intimidad ni a la privacidad, no requería resolución judicial habilitadora al efecto». Con ello convertía la toma de los datos contenido en un dispositivo de almacenamiento masivo en un aspecto que no necesitaba de autorización judicial al considerarlo amparado en la toma de un simple documento. También puede apreciarse una cuestión muy similar, que esta vez consiste en tomar un CD donde aparecía la grabación de una violación, usando para ello el auto que habilitaba para la entrada y registro y además sin la presencia del investigado por estar éste en otras entradas también ordenadas. STS 1045/2011, de 14 de octubre. Ponente: Don Juan Ramón Verdugo y Gómez de la Torre.

[352] SAP de Barcelona 288/2016, de 12 de junio. Ponente: Don José Grau Gasso. Esta sentencia, que cita otras del Tribunal Supremo y del Constitucional, resulta ilustrativa de la polémica que se genera con la entrada en domicilio y el acceso, una vez dentro de éste, a algún dispositivo electrónico encontrado en su interior, sea o no con consentimiento del afectado. Dice: «*En este sentido, la Sentencia de la Sala Segunda del Tribunal Supremo nº 444/2014 recuerda que conviene hacer referencia a la más reciente STC (Pleno) 115/2013, de 9 de mayo, que se refiere al acceso por parte de los agentes de la Policía Nacional, sin consentimiento del afectado y sin autorización judicial, a la relación de números telefónicos contenidos en la agenda de contactos telefónicos de un teléfono móvil (entendiendo exclusivamente por agenda el archivo del teléfono móvil en el que consta un listado de números identificados mediante un nombre) que fue encontrado por los agentes en el lugar de comisión de un delito, y considera que esta actuación no afecta al derecho al secreto de las comunicaciones (art. 18.3 CE) del usuario de dicho aparato de telefonía, sino exclusivamente al derecho a la intimidad (art. 18.1 CE)*.

Recuerda el Tribunal Constitucional que la intervención de las comunicaciones requiere siempre de autorización judicial, pero el ART. 18.1 CE no prevé esa misma garantía respecto del derecho a la intimidad, por lo que se admite la legitimidad constitucional de que la policía realice determinadas prácticas que constituyan una injerencia leve en la intimidad de las personas sin previa autorización judicial (y sin consentimiento del afectado), siempre que exista la suficiente y precisa habilitación legal y se hayan respetado las exigencias dimanantes del principio de proporcionalidad.

Estima el Tribunal Constitucional que con el acceso a la agenda de contactos del teléfono móvil del recurrente los agentes de policía no obtienen dato alguno concerniente a un proceso de comunicación emitida o recibida mediante dicho aparato, sino únicamente un listado de números de teléfono introducidos voluntariamente por el usuario del terminal, equiparable a los recogidos en una agenda de teléfonos en soporte de papel, por lo que debe descartarse que el derecho al secreto de las comunicaciones quede afectado por esta actuación policial.

Distinto sería el caso si se hubiese producido el acceso policial a cualquier otra función del teléfono móvil que pudiera desvelar procesos comunicativos, como por ejemplo el acceso al registro de llamadas entrantes y salientes.

……En todo caso, como ya hemos dicho, el acceso a las fotografías guardadas en el teléfono no requería de un previo consentimiento por parte del detenido, por lo que no cabe apreciar la vulneración del derecho fundamental invocado por la defensa de ……

Dicho consentimiento tampoco es necesario, en ausencia de resolución judicial, en el nuevo régimen introducido como consecuencia de la última reforma de la LECRIM, cuyo art. 588 sexies c) dispone que en los casos de urgencia en que se aprecie un interés constitucional legítimo que haga imprescindible la medida prevista en los apartados anteriores de este artículo, la Policía Judicial podrá llevar a cabo el examen directo de los datos contenidos en el dispositivo incautado, comunicándolo inmediatamente y en todo caso dentro del plazo máximo de veinticuatro horas al Juez competente para instruir la causa ….».

autorización judicial, y si la falta de alguno de estos elementos podría suscitar la vulneración en los derechos del afectado que determinase nulidad.

Abundando en esta misma idea, el párrafo segundo del art. 588 sexies a) LECrim establece que la mera incautación del dispositivo durante el registro domiciliario no habilita para poder acceder a la información contenida en el aparato intervenido. Para acceder al contenido de esa información se requiere una resolución judicial expresa y concreta que lo autorice.

En el auto que permita el registro del dispositivo deberán ser objeto de valoración, de manera autónoma y diferenciada, las razones que sean oportunas y que lleven a registrarlo. Estas razones deben de ser diferentes de las tenidas solo en cuenta para entrar en el domicilio. En realidad es que deben serlo, pues no cabe entender que sea igual el motivo que se tiene para entrar en una vivienda, que es buscar indicios del delito, que una vez dentro, los mismos argumentos permitan menoscabar otros derechos sobre los que el Juzgador no se pronunció, como la intimidad, por ejemplo.

No parece que exista ningún inconveniente para que los dos ejercicios o expresiones de la necesaria motivación se contengan en una sola resolución, pero lo verdaderamente importante es que se produzca una motivación distinta, separada y diferenciada para cada medida que se adopte. Pueden ser coincidentes en algún punto, pero lo que se busca por el legislador es que se motive la razón por la que es necesario entrar en el domicilio y separadamente las que sirven para registrar el dispositivo.

Esta exigencia de autorización motivada para registrar los datos contenidos en el dispositivo se contiene en el art. 588 sexies apartado b) LECrim, si bien, queda lógicamente desligada de la entrada en un domicilio, que es objeto de regulación diferenciada en otro apartado de la LECrim. El supuesto de hecho del que parte el precepto abarca únicamente el encuentro del dispositivo en cualquier lugar que no sea un domicilio. Por lo tanto, sólo bastará con dar cuenta al Instructor de este hallazgo, y se le solicite su registro para que valore si es necesario y proporcionado realizar el acceso y registro de los datos que pudiera albergar el dispositivo.

El registro de los datos debe ser ordenado, insistimos, judicialmente, sin que sirva cualquier clase de resolución, (es decir no puede adoptar la forma de providencia), sino que será una resolución debidamente motivada que sopese, analice y que exteriorice (a efectos de su ulterior control por parte de otros Tribunales, y por el mismo ciudadano en la vía de recursos) las razones que justifican en Derecho que se haya acordado el acceso al dispositivo de almacenamiento de datos pese a la afectación de derechos de rango constitucional detallados dentro del art. 18 de la Constitución, lo que conllevará necesariamente que adopte la forma de auto.

El concreto modo de acceso a los datos debe seguir los procedimientos y las directrices del art. 588 sexies apartado c. 1 LECrim[353]. Además, deben ser respetados tantos los presupuestos específicos que se exigen para su adopción, como los requisitos y principios comunes a todas las diligencias de investigación que están contempladas en el Capítulo IV del Título VIII, y que ya se han analizado.

Las exigencias legales contenidas del art. 588 sexies apartado c de la LECrim, no están enumeradas, sino que su concreto contenido debe ser extraído de la redacción de su enunciado. Estas exigencias pueden resumirse en tres aspectos: expresión del alcance del registro, empleo de los sistemas necesarios de salvaguarda de la integridad de los datos obtenidos, y garantía de preservación.

En primer lugar, se exige que la resolución judicial esté debidamente motivada y razonada (arts. 588 bis a), hasta 588 bis k) art. 588 sexies apartado c de la LECrim, en conjunción con el contenido del art. 588 sexies a o b LECrim. De manera que tiene necesariamente que ser explicada la fijación de los términos y del alcance del registro al dispositivo incautado[354]. Sobre estos puntos hay que tener en cuenta los siguientes aspectos:

a) Datos que no se incorporarán a la investigación.

El artículo apenas dice en qué deba consistir la motivación del auto sobre estos aspectos. En todo caso, parece que tiene que indicarse que los agentes que practiquen el registro, deberán excluir y obviar todos los datos que, estando en el interior del dispositivo, no guarden relación con todo o con parte de la investigación, o bien cuando se trate de datos que pertenezcan a terceros que no estén relacionados con ella o pertenezcan a su ámbito privado[355]. También se excluirán datos de naturaleza privada o que no tengan relación con la investigación, incluso cuando sean del investigado, o que de alguna manera resulten especialmente protegidos por otro derecho

[353] Dispone el mencionado párrafo 1 del art. 588 sexies, apartado c «*La resolución del juez de instrucción mediante la que se autorice el acceso a la información contenida en los dispositivos a que se refiere la presente sección, fijará los términos y el alcance del registro y podrá autorizar la realización de copias de los datos informáticos. Fijará también las condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación para hacer posible, en su caso, la práctica de un dictamen pericial».*

[354] Cfr. RODRÍGUEZ LAINZ, José Luis «¿Podría un juez español obligar a Apple a facilitar una puerta trasera para poder analizar información almacenada en un iPhone 6?». *Diario La Ley*, Nº 8729, 28 de Marzo de 2016. LA LEY 1356/2016 I. Pág. 4-5. Para el autor no se trata de una resolución al uso, sino que está limitada en aras a la protección del derecho al entorno virtual. Por ello RODRÍGUEZ LAINZ sostiene que: «*La misma resolución se encuentra sometida a unas especiales cautelas consecuencia del régimen privilegiado del conocido como entorno virtual; que comienza por la debida concreción del objeto y límites del registro, y termina con la restricción de las posibilidades de realización de copias, salvo expresa autorización judicial, o de su incautación física, salvo procedencia del decomiso o imposibilidad material de realización del examen durante la práctica de la diligencia de entrada y registro».*

[355] No importa el formato del dato de que se trate, sean fotografías, videos, textos, visitas a páginas web, audios, etc.

constitucional [356] , excluyendo, previamente cualquier relación de estos aspectos con la investigación[357].

Es bastante significativo la adjetivación que acompaña a la denominación de la diligencia, al aludir a un tipo de almacenamiento de datos efectuados con carácter "masivo". El adjetivo refiere abundancia o pluralidad desmedida, lo que nos debe llevar a la lógica consecuencia de descartar, entre tantos datos, aquellos que afecten a la intimidad de las personas, o los que no guarden relación con los hechos, o los que sean de terceros ajenos a la investigación. El pronunciamiento de este aspecto debe venir expresamente contemplado entre la motivación que le corresponde al Instructor.

En relación a los datos que deben quedar excluidos de la investigación, tendrá que ser el auto el que ofrezca los criterios para excluirlos de la investigación desarrollada, como también lo hace sobre otras cuestiones relacionadas con el registro de dispositivos de almacenamiento masivo. En la actualidad no se encuentra resoluciones que determinen qué tipo de criterios son los que pueden emplearse para expulsar de la instrucción los datos innecesarios, si bien si que puede hablarse de una paulatina adaptación de las resoluciones a la necesidad de introducir elementos que sirvan para discriminar el uso o no de determinados modos de actuación durante esta diligencia[358].

En todo caso la doctrina[359] va haciéndose eco de ciertos criterios jurisprudenciales que son proclives a admitir cierta amplitud en el registro, pero que lejos de verse justificada en aspectos arbitrarios,

---

[356] Puede ser el supuesto de alguna información que se encuadre en la relación abogado-cliente, En este sentido puede citarse la STS 79/2012, de 9 de febrero. Ponente: Don Miguel Colmenero Menéndez de Luarca, estableció citando alguna sentencia del TEDH sobre la relación abogado cliente que *«...el derecho, para el acusado, de comunicar con su abogado sin ser oído por terceras personas figura entre las exigencias elementales del proceso equitativo en una sociedad democrática y deriva del artículo 6.3 c) del Convenio. Si un abogado no pudiese entrevistarse con su cliente sin tal vigilancia y recibir de él instrucciones confidenciales, su asistencia perdería mucha de su utilidad (Sentencia S. contra Suiza de 2 noviembre 1991, serie A núm. 220, pg. 16, ap. 48). La importancia de la confidencialidad de las entrevistas entre el acusado y sus abogados para los derechos de la defensa ha sido afirmada en varios textos internacionales, incluidos los textos europeos (Sentencia Brenan contra Reino Unido, núm. 39846/1998, aps. 38-40, TEDH 2001-X)».* De estar ante archivos con estas características se debería desechar su contenido a los efectos de comprobar que se dan los requisitos que ahora se contienen en el art. 520.7 LECrim.

[357] Auto AP de Barcelona 214/2017, de 1 de marzo. Ponente: Doña Elena Guindulaín Oliveiras. El auto en su fundamento de derecho séptimo establece: «*Dando cumplimiento al mandato expreso del art. 588 sexies c de la LECRIM, la autorización de recabo de datos se limitará exclusivamente al examen de aquellas carpetas, archivos, ficheros o datos que puedan extraerse de la memoria física o virtual del dispositivo que pudieran tener una relación directa con los hechos objeto de concreta investigación en la presente causa»*.

[358] Auto del TSJ Madrid 50/2017, de 16 de mayo. Ponente: Don Francisco Javier Vieira Morente. El auto, que desestima un recurso de apelación interpuesto contra resolución dictada por Juzgado de Instrucción en el que se acordaba entrada y registro en domicilio, y volcado y análisis de dispositivos, vino a decir sobre el auto habilitan que: «*fijó los términos y el alcance del registro, identificando los terminales electrónicos a los que se refería la medida; analizó los indicios de la posible comisión de un delito y la utilidad del registro de esos dispositivos para lograr datos para su esclarecimiento; especificó la forma de realizar el volcado de información, con citación al investigado y a su letrado, así como en presencia del letrado de la Administración de Justicia»*. En el mismo sentido fáctico sirva de ejemplo el auto de la AP de Lugo, 315/2017, de 28 de marzo. Ponente: Doña Ana Rosa Pérez Quintana.

[359] Vid. RODRÍGUEZ LAINZ, José Luis. «Alcance de la medida de ingerencia y registro de dispositivo de almacenamiento masivo de datos. Comentario a la STS, Sala Segunda, de lo penal, 14-10-19». Base de datos SEPIN. SP/SENT/1020974.SP/DOCT/84003. Diciembre 2019. Pág. 3.

difusos o inconcretos deben guardar relación con el concreto hecho delictivo[360]. En todo caso deberá ser el transcurso del tiempo el que configurará otros criterios de inclusión o exclusión de datos, además de los estrictamente ajenos a la investigación.

b) Copia de los datos obtenidos.

El auto que autorice el registro del dispositivo de almacenamiento masivo también tendrá que pronunciarse sobre la necesidad de llevar a cabo copias de los datos informáticos. Es un aspecto que tiene mucha importancia, pues a diferencia de situaciones anteriores, en las que se privaba al dueño o usuario de los dispositivos encontrados durante todo el tiempo duraba la investigación, el párrafo segundo del mismo artículo exige en la actualidad, no privar al interesado del dispositivo, elevando esta consideración a fórmula general de conservación de los datos.

En todo caso esta regla general cede en la medida en que, para evitar esta privación del dispositivo, debe acreditarse ante el instructor, que se ocasione al privado del dispositivo alguna clase de perjuicio a la persona que es privada del dispositivo (por ejemplo, resulta más sencillo comprender los problemas que se causa si se incauta el servidor de una empresa, que si se incauta un lápiz de memoria). Por lo tanto, la manera de evitar el problema derivado de la privación del dispositivo es, que se ordene en el auto que habilite el registro, hacer una copia de estos. En todo caso se hacen ilimitadas las razones para justificar una aprehensión.

c) Condiciones a tener en cuenta para que los datos que lleguen a la causa sean los verdaderamente encontrados en el dispositivo y modo de asegurarlos.

La resolución judicial que acuerde la diligencia también indicará las condiciones que aseguren la integridad de los datos y las garantías necesarias para su preservación, de manera que los datos encontrados puedan servir como objeto de un examen pericial.

[360] STS 462/2019, de 14 de octubre. Ponente: D. Pablo Llarena Conde. La sentencia justifica el registro de datos ordenado en los teléfonos de varios de investigados por hechos constitutivos de un delito continuado de agresión sexual, en el hecho de que al tratarse de un caso en que el delito se consumó en un lugar en el que no había más testigos de los hechos que los que participaron en el mismo, los datos de toda índole que arrojasen los dispositivos podrían ayudar a comprender mejor cómo se dieron los hechos. La sentencia se refiere por lo tanto a los concretos contenidos que se podían registrar, asumiendo que podía accederse a todo en su totalidad, en ese supuesto. La justificación residía en la gravedad de los hechos, y en que los datos podrían arrojar mayor claridad a los mismos, y en que había existido una ponderación efectuada por un Juez.

Las formas de garantizar la integridad de los datos durante su obtención y posterior almacenamiento en el seno del proceso penal son muy variadas. Por ejemplo, existe la posibilidad de que el auto de autorización de la diligencia establezca la obligación de que la copia se haga en presencia judicial, o bien en presencia del Letrado de la Administración de justicia. Otras formas de garantizar la integridad de la información son, entre otras, las siguientes: imponer el deber de mantener la integridad de los datos al órgano encargado de la custodia del soporte donde los se almacenaba la información[361]; determinar el autor de autorización cual debe ser el mecanismo a emplear para el volcado de datos, o la copia de los mismos[362], etc.

En la práctica de nuestros tribunales, no obstante, esa diversidad de posibilidades de garantizar la integridad de los datos, sin embargo, y desde un punto de vista material, en las resoluciones que se están pronunciando sobre la materia no dejan de destacar que el nuevo precepto no exige ni la presencia del LAJ [363], así como tampoco del investigado[364].

3.2.1. Respeto a los presupuestos generales.

El contenido del art. 588 sexies, apartado c LECrim, no exige la observancia de más requisitos específicos que los que ya se han mencionado en páginas anteriores. En todo caso, esto no quiere decir que no tengan que cumplirse más exigencias, pues como en las demás diligencias a las que le

[361] Auto de la AP de Pontevedra 223/2017, de 21 de marzo. Ponente: Don José Juan Ramón Barreiro Prado. En esta resolución se pone de manifiesto que fue una medida acorde con el contenido del artículo 588 sexies c adoptar la diligencia de volcado de la información obtenida de un dispositivo de almacenamiento masivo de información, exigiendo la presencia del Letrado de la Administración de Justicia. Se aprecia así que se trata de un aspecto sobre los que el Juez instructor se puede pronunciar a la hora de establecer el cauce que asegure la integridad de los datos, su descarga y la realización de copias.

[362] Auto AP de Barcelona 214/2017, de 1 de marzo. Ponente: Doña Elena Guindulaín Oliveiras. Op. Cit. En el Fundamento jurídico séptimo puede leerse la forma que sepa tenido de reflejar el volcado de la información: «*Como garantía de la autenticidad e inalterabilidad de toda la información a la que se acceda durante el registro, deberán reflejarse en el acta que se realice cuantas actuaciones de acceso y examen se verifiquen, con apoyo si se estimara conveniente en el correspondiente soporte informático mediante la realización de copias de pantalla. Igualmente deberá realizarse una copia de seguridad, mediante volcado, de cuanta información fuera objeto de análisis ; la cual habrá de quedar bajo la custodia del Letrado de la Administración de Justicia que intervenga en el registro».*

[363] STS 165/2016, de 2 de marzo. Ponente: Don Alberto Jorge Barreiro. La sentencia destaca que el art. 588 sexies c) «*ni siquiera requiere la presencia del Secretario Judicial en el momento de abrir el ordenador y obtener el disco duro»*. Reitera este mismo aspecto la STS 213/2017, de 29 de marzo. Ponente: Don Carlos Granados Pérez, así como la STS 196/2017, de 24 de marzo. Ponente: Don Carlos Granados Pérez.

[364] SAN 6/2017, de 10 de marzo. Ponente: Don Fermín Javier Echarri Casi. La sentencia pone de manifiesto que durante el «*desprecinto y copiado de los datos informáticos, asistiendo a dicho acto el abogado del imputado ….., sin que constase en acta que hiciere manifestación de protesta alguna acerca de la no presencia del imputado como era su derecho, pero no un requisito legal al que se anude la legitimidad de la diligencia, por mucho que en la resolución habilitante así lo indique. Es más, ni la doctrina anterior en esta materia (jurisprudencia), ni la regulación llevada a cabo en la Ley de Enjuiciamiento Criminal por L.O 13/2015, de 5 de octubre (arts. 588 sexies a) a 588 sexies c) exigían la presencia del investigado como presupuesto material de su validez, máxime cuando su Letrado asistió a la misma, ya que ni el Instructor de oficio, ni la defensa interesaron se dejase sin efecto aquella, reiterando su práctica con la presencia del imputado».*

son exigibles, antes de la adopción de esta medida de investigación, se debe verificar que se han cumplido las exigencias del Capítulo IV, del Título VIII, relativas a las disposiciones comunes a todas las diligencias de investigación tecnológica.

En consecuencia, esto significa que, en aplicación de las reglas comunes, la resolución judicial, que acuerde el acceso y registro del dispositivo de almacenamiento masivo de información, deberá contener un ejercicio de valoración suficiente acerca de si en el caso concreto a la vista de los hechos investigados, puestos en relación con la petición de esta diligencia, se respetan los principios generales de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida, además del contenido exigido por el art. 588 bis c). 3 LECrim[365].

Es probable que los razonamientos que usaron inicialmente los investigadores se empleen nuevamente en la petición de la diligencia de registro de dispositivo de almacenamiento masivo[366], pero el Juez, por el contrario, ha de valorar de manera individualizada y específica las razones concretas que llevan a registrar el dispositivo en cuestión. La motivación que reciba la medida ha de ser específica, por lo tanto, el Juez deberá valorar las circunstancias del supuesto, el hallazgo encontrado en el domicilio, caso de haberse producido, el delito investigado, y la posibilidad de encontrar datos de un dispositivo de almacenamiento, cuyo contenido se desconoce.

Además, ha de tenerse en cuenta el contenido del principio de excepcionalidad, que prohíbe acudir a medidas gravosas cuando haya alguna otra de menor afectación o limitación de los derechos del investigado, y del principio de especialidad, que prohíbe las investigaciones prospectivas, sin relación con un delito concreto.

En especial, puede ser bastante útil detenerse en el tipo de delito que se está investigando, y en el modo en el que tal ilícito suela ejecutarse[367]. Realizar el acto de motivación en base al tipo penal que se esté investigando permite tomar las características propias de dicho tipo, y teniendo en

---

[365] Dispone el apartado 3 del art. 588 bis c que: «*3. La resolución judicial que autorice la medida concretará al menos los siguientes extremos: a) El hecho punible objeto de investigación y su calificación jurídica, con expresión de los indicios racionales en los que funde la medida. b) La identidad de los investigados y de cualquier otro afectado por la medida, de ser conocido. c) La extensión de la medida de injerencia, especificando su alcance así como la motivación relativa al cumplimiento de los principios rectores establecidos en el artículo 588 bis a. d) La unidad investigadora de Policía Judicial que se hará cargo de la intervención. e) La duración de la medida. f) La forma y la periodicidad con la que el solicitante informará al juez sobre los resultados de la medida. g) La finalidad perseguida con la medida. h) El sujeto obligado que llevará a cabo la medida, en caso de conocerse, con expresa mención del deber de colaboración y de guardar secreto, cuando proceda, bajo apercibimiento de incurrir en un delito de desobediencia».*

[366] Es momento de volver a recordar lo que ya se trató al analizar la propuesta de clasificación de las diligencias de investigación, y especialmente el carácter que esta diligencia tiene. Le atribuíamos un carácter derivado en tanto que lo característico de la diligencia de registro de dispositivos de almacenamiento masivo era, primero, encontrar el dispositivo, y posteriormente analizar su contenido. El carácter derivado se apreciaba en la medida en que se requería en la mayoría de los casos una diligencia de investigación previa a ésta.

[367] Por ejemplo, la modalidad comisiva de una estafa informática o de una falsedad documental admiten para su comisión el empleo de dispositivos electrónicos, cuyos datos deben quedar consignados en algún lugar. O bien son los datos empleados para realizar el acto, o bien por ejemplo son datos que ofrecen fechas, nombres, cifras, etc.

consideración dichos elementos es posible determinar si para apreciar la concurrencia de cada uno de ellos puede ser útil la medida de investigación electrónica de registro de dispositivos de almacenamiento masivo de información. Asimismo, acudir al modo concreto en que dicho tipo se ha ejecutado en el caso concreto también facilita relacionar su investigación con la diligencia analizada.

En todo caso, y pese a que los agentes pueden encontrar en ocasiones argumentos similares a los que sirvieron para la entrada y registro, en el caso de que ésta hubiera tenido lugar, el esfuerzo de razonamiento exigido a la policía judicial tampoco es simple. Los agentes encargados de la investigación expresarán qué es lo que puede ser útil para la investigación, porqué es conveniente acceder a los datos alojados en dispositivo encontrado, y qué razones hay para esperar que se encuentren en su interior dichos datos.

Como ya se ha señalado, nuevamente puede ser útil acudir al tipo de delito que se esté investigando para justificar la necesidad de la medida: así por ejemplo un delito de pornografía infantil, un delito de tráfico de drogas, son actos ilícitos en los que es habitual trabajar con datos informáticos, como las fotografías de los menores en clara actitud sexual, o los datos de los contactos que sirven como proveedores de sustancia o clientes de la misma en la cadena de compras. Además, debe tenerse en cuenta el contenido del art. 588 bis i) LECrim, puesto en relación con el art. 579 LECrim, para una eventual existencia de hallazgos casuales.

Los solicitantes ilustrarán al Juez Instructor sobre el modo en el que se realizará la diligencia, que deberá contar con un sistema que permita el acceso al dispositivo. Al respecto, podemos plantearnos qué sucede en el caso en el que el dispositivo tenga una clave o una contraseña para acceder a su contenido, lo que es cada vez más normal en la práctica [368]. La jurisprudencia se inclina por la necesidad de recabar un auto complementario, si es que la resolución habilitante inicial no hubiera dispuesto nada sobre este aspecto particular, que permita realizar las operaciones necesarias para acceder al contenido del dispositivo bloqueado.

[368] STS 97/2015, de 24 de febrero. Ponente: Don Juan Ramón Verdugo y Gómez de la Torre. El extenso fundamento jurídico cuarto de la sentencia se hace alusión al acceso a un ordenador, y una vez abierto el mismo a la necesidad de acceder a una red social para la que se necesitaba usuario y contraseña, que en este caso se consiguió solicitándose al propio investigado, que estaba presente en el registro domiciliario. En el caso se lo solicitó al investigado dicha clave y contraseña y la facilitó. Pero el Tribunal se plantea qué hacer en los casos en que no se obtenga dicha autorización, diciendo que «*Es cierto igualmente que el auto judicial por el que se decreta el volcado de datos informáticos contenidos en los ordenadores incautados no permite sin más el acceso a los contenidos de las redes sociales, sino que es preciso acceder a Internet e introducir una clave de usuario, por lo que apoderamiento del contenido de las redes sociales no se obtiene simplemente por el acceso al contenido del ordenador sino que requiere una acción adicional dirigida expresamente a su apertura y examen, siendo necesario el dictado de un nuevo mandamiento judicial*». Es pues claro que se necesita un auto judicial que habilite el acceso al dispositivo bloqueado, siempre que no se cuente con el consentimiento del afectado.

Los solicitantes además, informarán al Juez acerca de qué agentes ejecutarán la medida, del modo más concreto posible, según se desprende de la aplicación conjunta de los apartados 5º y 8ª del párrafo segundo del art. 588 bis b LECrim. Una solicitud bien fundamentada y completa otorga mucha mayor seguridad a los datos que son finalmente entregados para que formen parte de la investigación, así como también fortalece el resultado de su análisis y estudio.

El auto judicial que se dicte sobre la diligencia de acceso y registro de datos de un dispositivo, a diferencia de la relativa a las intervenciones de comunicaciones, que *"se dictará en un plazo de veinticuatro horas desde que se presente la solicitud»*, no está sometida a plazo, pues se trata de una medida que se ejecuta con el mero análisis[369]. En todo caso si que requiere previa audiencia del Ministerio Fiscal, que deberá pronunciarse sobre la oportunidad de la diligencia de acceso a dispositivo de almacenamiento masivo.

El contenido de esta diligencia, como cualquier otra de las contenidas en la LECrim, cumplirá con el contenido del artículo 588 bis, d, LECrim, conforme al cual, la pieza en que se sustancie el contenido de esta diligencia será separada y secreta, sin que tal declaración tenga porqué resultar siempre necesaria para la totalidad de la causa. Esta pieza, según doctrina, *«la abre la mera solicitud y no el auto por el que se acuerda interponer la medida»*[370].

Los datos que sean obtenidos a consecuencia de esta diligencia serán debidamente conservados, si bien reservando exclusivamente los que tengan interés para la causa. Toda la información que no reúna esa condición de interés o necesidad, o que afecte a terceros ajenos al proceso, números de teléfono, mensajes de SMS, correos electrónicos, fotografías y videos, datos económicos derivados de haber efectuado alguna operación de compra por internet o datos bancarios, tendrán que ser eliminados de la copia cuando lo disponga el auto.

Es necesario tener en cuenta a los efectos de un análisis integral de esta diligencia que estas disposiciones que regulan la diligencia parten del contenido del art. 588 bis h) LECrim. En este sentido hay que recordar que este precepto somete la posible afectación de terceros a la regulación específica que en cada una de las diligencias de investigación se pudieran adoptar, en el supuesto de esta diligencia de investigación concreta, no se ha regulado ninguna medida específica sobre la

---

[369] Auto Audiencia Provincial de Álava, sección segunda, 255/2018, de 9 de mayo de 2018. Ponente: Doña Ana Jesús Zulueta Álvarez. La resolución expresa la innecesariedad de someter a plazo esta diligencia, contraponiéndola a la exigencia a sometimiento temporal que sí que afecta a la diligencia de intervención de comunicaciones, diciendo sobre esta última que *«Esta diferencia en la regulación es lógica ,atendiendo a la diferente naturaleza de los objetos regulados. La intervención telefónica es dinámica e implica una limitación de los derechos fundamentales, que por su propia naturaleza se prolonga en el tiempo*».

[370] BUENO DE MATA, Federico. *Las diligencias de investigación penal en la cuarta revolución industrial. Principios teóricos y problemas prácticos.* Aranzadi. Navarra. 2019. Libro electrónico no paginado (Capítulo I, apartado III).

afectación de información de terceras personas. Por lo tanto, lo más lógico será apartar de la causa cualquier dato que no sea indispensable[371] para la investigación cuando contenga información sobre terceras personas ajenas a la misma. Se sigue, por lo tanto, un criterio restrictivo a la hora de incluir en las actuaciones, los datos de terceros, al igual que también debe prevalecer un principio limitativo a la hora de privar al afectado del dispositivo que contenía la información, tal y como corrobora el contenido del párrafo 2, del art. 588 sexies c) LECrim, aunque para ello se requiere que se cause perjuicio a su titular [372].

En todo caso, dada la heterogeneidad de los datos que se pueden localizar dentro de un dispositivo de esta naturaleza, hubiera sido deseable que el legislador especificase qué hacer cuando aparezcan datos que puedan ser investigados mediante otra diligencia de investigación distinta o mucho más específica[373].

La ausencia de una disposición concreta sobre esta concreta cuestión ha de ser suplida con la necesidad de una motivación reforzada en el auto, o bien a un complemento del mismo, y en la que especialmente se desarrolle debidamente la aplicación del principio legalidad, en la medida en que será de aplicación preferente aquélla diligencia que cuenta con regulación especial, así como la aplicación del principio de proporcionalidad, porque deben ser atendidas todas las circunstancias del caso en concreto, y analizados todos los hechos será necesario ponerlos en relación con la medida que en ese caso pudiera afectar a más de un derecho del art. 18 CE.

Como solución a esta situación, me decanto por acudir a la solicitud de complemento del oficio policial para que éste sea el que clarifique, dentro de lo posible, de qué tipo de dispositivo se trata, y si es posible que el mismo contenga datos referentes a comunicaciones vivas, porque de serlo es necesario seguir la diligencia aplicando las disposiciones relativas a las intervenciones de esta naturaleza.

En suma, se deben adoptar las garantías que fuesen necesarias para evitar cualquier clase de nulidad[374], lo que convierte tanto al oficio policial, como al auto judicial, en los elementos

[371] El art. 588 sexies b utiliza dicho adjetivo a los efectos de autorizar el acceso a la información contenida en el dispositivo.
[372] Vid. MARCHENA GÓMEZ, GONZÁLEZ CUELLAR- SERRANO. Op. cit. Pág. 377-378.
[373] Por ejemplo, hubiera sido útil que la ley determinara qué hacer en los casos en que dentro de un dispositivo aparezcan datos que se podrían obtener empleando para investigarlos una diligencia de intervención de comunicaciones, o una apertura de correspondencia, como por ejemplo cuando se tratase de datos contenidos en un router o un dispositivo similar en el que queden rastros de comunicaciones aún no finalizadas. Cabe plantearse qué diligencia es la que debe seguirse en estos casos, la de registro de dispositivo de almacenamiento masivo, o bien la específica por razón de la materia que afecta.
[374] Por ejemplo, dar con correos electrónicos que aún no se han leído, lo que haría conveniente que el investigado estuviera presente a los efectos de su apertura como si se tratara del correo físico ex art. 579 LECrim.

esenciales que, respectivamente, ofrecen información suficiente, y valoran las circunstancias concurrentes.

3.3. El acceso a repositorios de datos.

La regulación que realiza el art. 588 sexies, en sus distintos apartados, desglosa el modo en que se accede, generalmente, a los dispositivos que contienen información. No obstante, se impone una exégesis exclusiva del contenido del párrafo tercero del artículo 588 sexies c) LECrim[375], porque contempla de manera diferenciada una clase de accesos y registros que, por sus propios elementos, presenta una serie de características que las diferencia y la distingue, de los accesos y registros generales.

Este artículo describe un supuesto de hecho diferente al de los dos primeros artículos del Capítulo VIII, aunque está claramente relacionado con ellos. El supuesto de hecho del que parte el precepto es el de un acceso y registro de información que ya ha sido previamente autorizado, y que aparece

---

[375] Se hace necesario, a los efectos de facilitar una mejor lectura y comprensión del apartado, transcribir el precepto, que dice textualmente lo siguiente: «*Artículo 588 sexies c. Autorización judicial. 1. La resolución del juez de instrucción mediante la que se autorice el acceso a la información contenida en los dispositivos a que se refiere la presente sección, fijará los términos y el alcance del registro y podrá autorizar la realización de copias de los datos informáticos. Fijará también las condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación para hacer posible, en su caso, la práctica de un dictamen pericial. 2. Salvo que constituyan el objeto o instrumento del delito o existan otras razones que lo justifiquen, se evitará la incautación de los soportes físicos que contengan los datos o archivos informáticos, cuando ello pueda causar un grave perjuicio a su titular o propietario y sea posible la obtención de una copia de ellos en condiciones que garanticen la autenticidad e integridad de los datos. 3. Cuando quienes lleven a cabo el registro o tengan acceso al sistema de información o a una parte del mismo conforme a lo dispuesto en este capítulo, tengan razones fundadas para considerar que los datos buscados están almacenados en otro sistema informático o en una parte de él, podrán ampliar el registro, siempre que los datos sean lícitamente accesibles por medio del sistema inicial o estén disponibles para este. Esta ampliación del registro deberá ser autorizada por el juez, salvo que ya lo hubiera sido en la autorización inicial. En caso de urgencia, la Policía Judicial o el fiscal podrán llevarlo a cabo, informando al juez inmediatamente, y en todo caso dentro del plazo máximo de veinticuatro horas, de la actuación realizada, la forma en que se ha efectuado y su resultado. El juez competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de setenta y dos horas desde que fue ordenada la interceptación. 4. En los casos de urgencia en que se aprecie un interés constitucional legítimo que haga imprescindible la medida prevista en los apartados anteriores de este artículo, la Policía Judicial podrá llevar a cabo el examen directo de los datos contenidos en el dispositivo incautado, comunicándolo inmediatamente, y en todo caso dentro del plazo máximo de veinticuatro horas, por escrito motivado al juez competente, haciendo constar las razones que justificaron la adopción de la medida, la actuación realizada, la forma en que se ha efectuado y su resultado. El juez competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de 72 horas desde que fue ordenada la medida. 5. Las autoridades y agentes encargados de la investigación podrán ordenar a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo que facilite la información que resulte necesaria, siempre que de ello no derive una carga desproporcionada para el afectado, bajo apercibimiento de incurrir en delito de desobediencia.Esta disposición no será aplicable al investigado o encausado, a las personas que están dispensadas de la obligación de declarar por razón de parentesco y a aquellas que, de conformidad con el artículo 416.2, no pueden declarar en virtud del secreto profesional*».

como necesario para la investigación en el cuero de una fase en la que se está produciendo el análisis de los datos. Durante el desarrollo de este análisis es cuando aparece una nueva ubicación, en la que pueden encontrarse radicados más datos de utilidad e interés para la causa.

La diferencia con los casos anteriores es que, en este último caso, los datos no están en el dispositivo físico, sino en una red o directamente en la nube, o en lo que el texto legal denomina, sistema informático.

Es por eso por lo que se le otorga por parte del legislador un tratamiento separado del registro habitual, y dentro del párrafo tercero, se regula la diligencia de acceso a la información, alojada en un «*sistema informático»*, bien de modo total o parcial.

Lo primero que debe analizarse es la definición de un sistema informático, que no es más que el «*conjunto de procesos formales, interdependientes y ordenados que actuando sobre bases de datos consiguen facilitar información, transformar los procesos, transformar la organización, y ayudan a implantar nuevas estrategias»* [376]. La Ley se decanta por expresiones como "*repositorio de datos*" o "*sistema de información*", tratándose tan sólo de acepciones técnicas y algo confusas. En todo caso, el texto se refiere de maneras diferentes al mismo objeto, pues mientras en el apartado 1 habla de *"repositorios de datos"*, en el 3 se habla de "*los datos buscados están almacenados en otro sistema informático o parte de él*". Las acepciones de sistema de información, sistema informático y repositorios son categorías poco habituales para los no versados, pero el texto de la Ley parece referirse a ellos para nombrar a lo mismo, esto es, una ubicación distinta al propio dispositivo físico.

En realidad, el supuesto de hecho puede parecernos diferente al que está regulado por los artículos anteriores, pero no es así. Lo que hace el legislador es tratar del mismo modo tanto el registro de un dispositivo físico, como el acceso a la información almacenada en espacios virtuales. Teniendo presente que la finalidad que persigue esta diligencia es obtener datos electrónicos, no hubiera tenido sentido regular tan detalladamente el acceso a los dispositivos físicos y olvidar toda mención a los servicios en la nube, que, pese a que no son dispositivos tangibles, cumplen con la misma función. Para el legislador no hay diferencia que justifique tratar de manera distinta a un objeto físico que contiene información que a aquél sistema que se encarga del alojamiento de información en la nube. De hecho, no debe perderse de vista que la Ley sólo acude y usa el término dispositivo, palabra que, según el Diccionario de la Real Academia, es el sustantivo que se refiere a un «*mecanismo o artificio para producir una acción prevista»*. En este caso, como la acción prevista

[376] Cfr. GINER DE LA FUENTE. Fernando. *Los sistemas de información en la sociedad del conocimiento*. ESIC. Madrid. 2004. Pág. 35 y 46. De entre los elementos de un sistema de información el autor destaca los datos, el hardware, el software, las bases de datos, las redes de comunicaciones y las personas.

es la obtención de información, es indiferente dónde se haya colocado la misma, bien sea en un artefacto físico o bien en un servicio virtual.

En suma, el legislador equipara la salvaguarda virtual de información como si de un dispositivo más se tratara, acogiendo un concepto de dispositivo muy amplio, que abarca desde un mero artefacto físico a todo un sistema informático. Se trata de una verdadera actualización de la concepción legal sobre dispositivos que sirven para guardar información, abarcando modalidades, servicios y sistemas que ofrecen la misma función que un dispositivo físico y tangible: servir de contenedor de información. La diferencia que hay entre ellos no está tanto en la finalidad que cumple cada tipo de alojamiento de la información, como en el modo de acceso a cada tipología, porque cuando el dispositivo es virtual, hay que encontrar un método para llegar hasta la información, diferenciando el lugar donde están alojados los datos, del aparato que se usa para acceder a ella. Nuestra actual legislación considera que tanto un dispositivo físico como uno virtual son susceptibles de ser registrados, pero la verdadera diferencia entre las dos tipologías de registro reside en que en el caso en que el dispositivo es físico, los requisitos son mucho más sencillos de aplicar, mientras que cuando estamos ante el registro de un dispositivo virtual las exigencias son mayores, e incluso se complican llegado el caso en que los datos están ubicados fuera del territorio nacional.

En estos últimos casos, la legislación procesal española, incluso tras haber sido reformada incurre en falta de claridad y concreción. Pero incluso existen algunos problemas, derivados del marcado carácter técnico de los dispositivos en los que se guarda la información, en los que cabe dudar si estamos ante un dispositivo físico, o bien uno virtual.

La regla que sirve en este supuesto es que todo dato que se encuentre en el interior del ordenador y que no requiera ser buscado fuera del mismo, puede ser obtenido mediante la aplicación de la diligencia de registro dispositivo que ya hemos visto. Por el contrario, si la información está más allá del apartado encontrado, debe seguirse el contenido de la diligencia de registro contenida en el este apartado.

La amplitud con la que se refiere el precepto legal al concepto de sistema permite una gran variedad de situaciones, incluyendo una cierta capacidad de ajustarse a los nuevos sistemas de almacenamiento de información que la técnica pudiera ir desarrollando. Por ejemplo, los datos que pudieran estar alojados en servidores de una empresa o una organización que esté siendo investigada, el servidor empleado directamente por el investigado, o los servicios en la nube a los que se accede mediante internet. Todos estos son ejemplos de sistemas de información, ajenos al

dispositivo, pero que se emplean como puerta de acceso al mismo[377], y con la nueva regulación se permite el acceso a todos ellos.

El antecedente más inmediato de esta diligencia, tal y como ya se ha dicho, se encuentra en el Convenio sobre Ciberdelincuencia, que contiene una medida similar en su artículo 19.2[378]. La redacción que ofrece el Convenio, comparada con la nuestra, es muy similar, siendo el contenido del art. 588 sexies c, párrafo 3 LECrim, en algunas de sus líneas, casi idéntico. El artículo 19 del Convenio, establece, en su apartado primero, la obligación de los países firmantes, de legislar sobre la autorización de registro en dos situaciones distintas.

La primera se refiere a *«un sistema informático o a una parte del mismo, así como a los datos informáticos almacenados en el mismo»*, y la segunda situación que se contempla en el registro en «*un medio de almacenamiento de datos informáticos».*

En el apartado segundo del mencionado artículo del Convenio, se prevé el caso en que se parte de un registro de un dispositivo ya en curso, como el supuesto previsto en el art. 588 sexies c.3, y durante el mismo aparece la posibilidad de que existan datos en un sistema informático, distinto al autorizado inicialmente. Esta ubicación distinta justifica, según el tenor del Convenio, legislar para que se obtenga, de manera rápida, la autorización necesaria para registrar dentro de la nueva localización. La norma internacional no prohíbe que la autorización pueda venir prevista en la autorización inicial. En este sentido, no se debe perder de vista que la ley española permite, expresamente, que en el auto se incluyan ambas situaciones[379].

---

[377] Vid. RODRÍGUEZ LAINZ, José Luis. «Tres cuestiones polémicas sobre el registro de dispositivos electrónicos de almacenamiento masivo de información». *Base doctrinal ed. SEPIN*. Nº Documento SP/DOCT/21066. Septiembre 2016. Págs. 2 y 3. El autor en este artículo nos ofrece otro interesante ejemplo de lo que puede entenderse como "sistema de información". Nos ofrece la posibilidad de que pueda entenderse por tal el acceso a la red interna o servidor de una empresa en la que se guardan los datos de un determinado hecho. Por otro lado, también sostiene la posibilidad de que la información se encuentre alojada en un sistema gestionado por un tercero.

[378] El tenor literal de la norma dispone: «*2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para asegurar que, cuando sus autoridades procedan al registro o tengan acceso de una forma similar a un sistema informático específico o a una parte del mismo, de conformidad con lo dispuesto en el apartado 1.a, y tengan razones para creer que los datos buscados están almacenados en otro sistema informático o en una parte del mismo situado en su territorio, y dichos datos sean lícitamente accesibles a través del sistema inicial o estén disponibles para éste, dichas autoridades puedan ampliar rápidamente el registro o la forma de acceso similar al otro sistema*". Por su parte el art. 588 sexies, c, 3 dispone que: "*Cuando quienes lleven a cabo el registro o tengan acceso al sistema de información o a una parte del mismo conforme a lo dispuesto en este capítulo, tengan razones fundadas para considerar que los datos buscados están almacenados en otro sistema informático o en una parte de él, podrán ampliar el registro, siempre que los datos sean lícitamente accesibles por medio del sistema inicial o estén disponibles para este. Esta ampliación del registro deberá ser autorizada por el juez, salvo que ya lo hubiera sido en la autorización inicial. En caso de urgencia, la Policía Judicial o el fiscal podrán llevarlo a cabo, informando al juez inmediatamente, y en todo caso dentro del plazo máximo de veinticuatro horas, de la actuación realizada, la forma en que se ha efectuado y su resultado. El juez competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de setenta y dos horas desde que fue ordenada la interceptación».*

[379] La búsqueda de datos bien sea en un dispositivo físico o en uno virtual descansan en una misma finalidad y en un mismo proceso de razonamiento, y por lo tanto no hay razón para que un auto que se pronuncia sobre dicho registro, deje prevista las dos opciones.

El Convenio no incluye la expresión *«repositorio telemático de datos»*, que sí está previsto en el art. 588 sexies a 1 LECrim. La norma española relaciona los diferentes dispositivos que se pueden registrar, siendo en este sentido mucho más concreto que el Convenio. El Convenio puede referirse al repositorio en su art. 19.2, si bien de manera distinta al referirse *«a un medio de almacenamiento de datos informáticos en el que puedan almacenarse datos informáticos»*.

En suma, lo que permiten los legisladores tanto nacionales, como los redactores del convenio es el registro de un artefacto tangible, el de redes físicas que unen dispositivos entre sí, y el acceso a los datos alojados en la nube, o en servidores externos.

En este último aspecto, el del acceso a datos alojados en sistemas virtuales, el 588 sexies c, párrafo 3 LECrim, permite registrar el contenido de un sistema informático, considerándolo como un segundo registro, o como una diligencia *ex post*. Es decir, el legislador regula este registro de los datos alojados en sistemas virtuales como una hipotética respuesta legal derivada de la información que pudiera encontrarse tras la realización de un acceso a un dispositivo de almacenamiento masivo de datos, en la que se aprecie la necesidad de tener que acudir a uno de estos sistemas de almacenamiento, por existir sospechas de que en ellos se aloja información de interés para la investigación[380]. En todo caso, nuestra norma sí que permite que en el auto inicial se prevea esta autorización, sin necesidad de que se necesite un nuevo auto, o que se haya producido un registro previamente, pues estos extremos pueden venir contemplados por el Instructor. No obstante, los investigadores deberían hacer saber al Juzgador de esta posibilidad, para que en el auto se diera una respuesta específica.

En segundo lugar, el art. 19.2 del Convenio, y también la LECrim, exigen que los «*datos sean lícitamente accesibles por medio del sistema inicial o estén disponibles para este»*. Esta expresión, sobre todo en su último inciso, es compleja, controvertida y poco transparente. El precepto admite diversas formulas de interpretación jurídica, y también de aplicación efectiva, así como se usan vocablos que admiten diferentes significados, algo indeseable dentro del ámbito de la instrucción penal, donde rige la reserva de ley, la protección de los derechos de los investigados (bajo el manto del principio de presunción de inocencia), y que exige que los procesos de investigación estén legalmente previstos. El contenido del Convenio tiene una redacción que bien pudo haber sido aclarada o corregida por el legislador español al insertarla en la normativa procesal interna (art. 588 sexies c, apartado 3 LECrim).

---

[380] Por ejemplo, cabe pensar en que tras registrar un router se encuentren numerosos accesos a un servidor bajo contraseña, de esto puede sospecharse que en este servidor se encuentra información distinta a la encontrada en el dispositivo registrado, y por ello se requiere la ampliación del registro para saber qué información se contiene en dicho lugar.

Una posible interpretación del supuesto de hecho admite el acceso a unas bases de datos, repositorio o sistema de información, o el acceso a servidores de terceros, cuando este acceso es lícito para el investigado[381]. Es decir, que si el investigado puede acceder lícitamente, los investigadores también pueden. En todo caso no se explica qué es para el legislador un acceso lícito, porque normalmente lo será aquél en el que haya usuarios acreditados o haya una contraseña.

Otra interpretación, más restrictiva, admite también ese acceso lícito, sólo cuando la puesta en marcha del dispositivo ya conecta por sí sola con estas redes o servicios virtuales, sin necesidad de realizar ninguna otra tarea u operación adicional.

La interpretación más admisible, atendido el tenor legal es, a nuestro juicio, la que admite el acceso y registro sólo cuando el acto de acceso a la información se realiza sin necesidad de hacer ninguna operación que exija una interacción informática por parte de otra persona ajena al usuario. La expresión «*lícitamente»* debe interpretarse en el sentido de que se realiza de modo que no hace falta que intervenga ni el investigado ni los investigadores[382].

La licitud de la medida depende de que el sistema de acceso y registro esté previsto en la ley, circunstancia ésta que se ha visto colmada en nuestra legislación precisamente con la regulación de esta diligencia. Esta carencia se suple pidiendo autorización judicial que permita a los agentes el registro de un dispositivo o bien de un sistema informático que requiera clave.

La expresión «*o estén disponibles para este»* es aún de más difícil comprensión, ya que admite diversas interpretaciones, alguna incluso más atrevida y arriesgada que las que permite la anterior expresión. La disponibilidad es definida como aquello de lo *«que se puede disponer libremente de ella o que está lista para usarse o utilizarse»*[383]. Por lo tanto, en la definición legal se contemplan sólo métodos de acceso que supongan una entrada libre a la información.

El problema del acceso desaparece cuando el investigado aporta las claves para realizarlo[384], porque su consentimiento suple la vulneración del derecho afectado. Sin embargo, cuando el investigado no

---

[381] Vid. RODRÍGUEZ LAINZ, José Luis. "Tres cuestiones polémicas sobre el registro de dispositivos electrónicos de almacenamiento masivo de información". Op. Cit. Pág. 1 y 2. Esta es la interpretación que defiende el autor, un acceso a tales repositorios que son accesibles lícitamente para el investigado.

[382] Ibídem «*Tanto en los alojamientos que pudiéramos definir como convencionales como en los alojamientos en la nube, lo primordial será la posibilidad de un acceso legítimo a través del dispositivo; lo cual, aparte del ejemplo del consentimiento del interesado, puede tener lugar tanto cuando en el curso del registro se descubre un enlace o link que facilita un acceso directo a tales alojamientos como cuando se consiguen desvelar las claves de acceso a determinados perfiles de redes sociales, posiblemente relacionados con el objeto de la indagación. Obviamente, la utilización de una clave de usuario no es un baluarte inexpugnable que cierre el acceso a un registro legalmente autorizado»*.

[383]Definición obtenida de la edición digital del DRAE http://dle.rae.es/?id=DxfA3tW

[384] SAP Zaragoza, sección 6º, 164/2018, de 12 de junio. Ponente: Don Rubén Blasco Obede. La sentencia versa sobre el enjuiciamiento de varios delitos contra la indemnidad sexual de menores de edad, entre ellos elaboración de materia de pornografía infantil. Se aprecia en los hechos como fueron encontrados varios instrumentos, entre ellos un móvil con acceso a DROPBOX en el que se contenían esas fotos. En este supuesto no se cuestiona el acceso porque las claves las dio el afectado, colaborando así con el esclarecimiento de los hechos.

las facilita surge el inconveniente de cómo llegar hasta los datos. El concepto de disponibilidad debe implicar que para ejecutar el acceso a los datos no es necesario hacer nada especial. Es decir, abrir el ordenador y acceder, sin más, al lugar en el que se guardan esos datos. Sólo cuando para efectuar el acceso no se dispongan de las claves es cuando habrá que buscar otras formas de acceder, y son precisamente las que no se clarifican en la ley. Hasta el momento, del contenido de alguna resolución judicial, parece que la práctica de la instrucción suele decantarse, en estos casos, por oficiar a las empresas proveedoras de los servicios para que aporten estos datos[385].

El precepto también admite otro tipo de entendimiento, que incluiría usar alguna clase de sistema que permitiese "abrir" el acceso a tales servicios para hacerlos disponibles. En todo caso se impone hacer una interpretación lo más acorde posible a la tutela de derechos fundamentales, y realizarla de este modo se hace más urgente que en otra clase de diligencias, porque ésta permite que, de modo excepcional y urgente, se ordene la toma de datos por la policía judicial, o por el Fiscal, informando al juez en el breve plazo de veinticuatro horas sobre ello para que ratifique o rechace la medida.

La insuficiente claridad legal puede derivar en la aparición de nuevos problemas de vulneración de derechos fundamentales, o incluso que terminen usándose métodos de acceso a los datos que no están previstos en la ley. Hubiera sido deseable una mayor pulcritud técnica a la hora de tipificar el acceso a los datos almacenados en repositorios, sistemas informáticos y dispositivos virtuales, desechando cualquier laguna interpretativa sobre el acceso a un dispositivo virtual sin clarificar el modo de hacerlo. No obstante, será el desarrollo de la jurisprudencia, el que vaya ilustrando el modo correcto de entender estos casos.

3.4. Autorización no judicial por razones de urgencia. Imposición de obligaciones de conservación a terceros.

El párrafo cuarto del artículo 588 sexies apartado c, párrafo 4 LECrim[386], contiene la facultad de acceso y registro al contenido de un dispositivo, de forma inmediata y directa. Se requiere para ello que las circunstancias justifiquen este acceso, lo que sólo cabe cuando se trata de proteger un

[385] Es el supuesto que se contempla en los hechos de la SAP de Madrid, sección 30, 316/2018, de 3 de mayo. Ponente: Doña Inmaculada López Candela.

[386] El apartado dispone expresamente que: «*4. En los casos de urgencia en que se aprecie un interés constitucional legítimo que haga imprescindible la medida prevista en los apartados anteriores de este artículo, la Policía Judicial podrá llevar a cabo el examen directo de los datos contenidos en el dispositivo incautado, comunicándolo inmediatamente, y en todo caso dentro del plazo máximo de veinticuatro horas, por escrito motivado al juez competente, haciendo constar las razones que justificaron la adopción de la medida, la actuación realizada, la forma en que se ha efectuado y su resultado. El juez competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de 72 horas desde que fue ordenada la medida*»

«i*nterés constitucional legítimo»*. La norma no se detiene en detallar cuál es el interés constitucional o legítimo, lo cual hubiera sido deseable, dejándose a la interpretación y motivación judicial en el auto que ratifique la medida ejecutada por razones de urgencia.

La ausencia de definición de la relevancia constitucional puede suplirse considerando que tal presupuesto habilitante concurre en todas aquellas situaciones en las que puedan estar en peligro bienes jurídicos que tienen protección constitucional: la vida, la integridad física y moral, el patrimonio, la salud, la necesidad de evitar un delito en el acto, etc. Una interpretación similar a esta es la que sigue la Fiscalía General del Estado, que añade también aspectos propios de la seguridad nacional, el bienestar del país, etc[387].

En todo caso, en una cuestión tan sensible, hubiera sido deseable cierta concreción, no tanto por el hecho de que resulte complicado saber qué tipos de intereses constitucionales son los que refiere el precepto, sino porque son los agentes de la autoridad los que están facultados legalmente para realizar esta intervención y registro amparados en razones de urgencia, y queda a su exclusivo arbitrio la decisión inmediata de apreciar el riesgo para tales intereses constitucionales. Se trata de una intromisión en los derechos constitucionales que está admitida por la Ley, pero que se hace sin cobertura judicial previa, dejándose a la subjetiva apreciación de los agentes verificar su concurrencia.

Una vez producida dicha circunstancia de urgencia, y producido el acceso y registro de los datos por la policía judicial, o bien por orden del Fiscal, se debe comunicar al Juez este hecho inmediatamente. En esa comunicación se detallarán las razones de la decisión adoptada en atención a la urgencia de las circunstancias concurrentes. Debe entenderse, en la lógica del acontecimiento producido, que los que hayan efectuado este acceso habrán de detallar cuál ha sido el contenido de los datos recabados, cómo se llevó a cabo ese acceso y la utilidad que esto haya reportado, pero sobre todo explicarán las concretas razones de urgencia apreciadas, y la posible lesión a un derecho constitucional. La comunicación-justificación debe producirse en el plazo de veinticuatro horas desde que se realizó la toma de los datos y el registro del dispositivo[388]. La autoridad judicial deberá revocar o confirmar la medida ejecutada por razones de urgencia, mediante otra resolución

[387] Circular de la Fiscalía General del Estado 5/2019, de 6 de marzo, que cita a su vez a la Circular de la Fiscalía General del Estado 1/2013, de 6 de marzo de 2019. Pág. 44

[388] Criterio seguido también en la CFGE 5/2019, de 6 de marzo. Pág. 45. Dicha Circular menciona la necesidad de realizar una diligencia de constancia en la que se consigne la hora exacta de esta acción, para que el Juez pueda comprobar si los plazos se han respetado.

motivada que se dictará en plazo de setenta y dos horas, que también han de contarse desde la realización del registro[389].

En otro orden de cosas, y más concretamente en las obligaciones que la ley impone a terceros, durante la práctica de esta diligencia, hay que referirse al contenido del párrafo quinto del artículo 588 sexies c LECrim. Este precepto impone a «*cualquier persona»* que conozca el funcionamiento de un sistema informático, o las medidas de protección de los datos contenidos en el sistema informático, una obligación general consistente en proporcionar la información que sea necesaria para acceder a ellos. El obligado podrá incurrir en la comisión de un delito de desobediencia si incumple esta obligación. Esta imposición no alcanza, en ningún caso, ni al investigado, ni a sus allegados, ni a cualquier persona que disfrute de la dispensa de la obligación de declarar por razones de parentesco, o por razones de secreto profesional, conforme al art. 416.2 LEcrim[390]. Es una obligación que presenta un contenido muy similar al que se exige en la regulación expresa de otras diligencias de investigación[391].

La imposición de esta clase de obligación está justificada en la volatilidad y vulnerabilidad de los datos contenidos en dispositivos de almacenamiento masivo. Por eso, se obliga a aquél tercero ajeno a la investigación, que sabe cómo extraerlos o mantenerlos seguros, que impida cualquier tipo de

[389] Cfr. RODRÍGUEZ LAINZ, José Luis. «Tres cuestiones polémicas sobre el registro de dispositivos electrónicos de almacenamiento masivo de información». Op. Cit. Pág. 5. El autor realiza una distinción entre esta posibilidad de acceso inmediato por razones de urgencia, de la llamada orden de conservación de datos contenida con carácter general en el art. 588 octies de la LEcrim. Compara ambas medidas y considera que «*Desde el mismo momento en que exista un riesgo cierto y elevado de destrucción o desaparición de la información mientras se emite y recibe por el destinatario la orden de retención, incluso por parte de este, sería absolutamente legítima la opción por la vía del acceso directo a tal información con posterior ratificación judicial, preferentemente»*. Por lo tanto, sostiene que la medida del art. 588 sexies, resulta más aplicable a situaciones de urgencia que la orden de conservación. Es por ello por lo que sigue diciendo que «*Descubierta la nueva fuente accesible a través del sistema inicial existe un alto riesgo de eliminación por personas que pudieran colaborar con el sujeto investigado; o incluso dudar de la fiabilidad de quien gestiona el almacenamiento de datos propios de la persona investigada; y la preparación, emisión y recepción de la orden de retención podrían dar lugar a un espacio de tiempo más que suficiente como para que tales personas reaccionaran eliminando o haciendo inaccesible dicha información».* En todo caso se trata de una cuestión que debe apreciarse bajo la óptica de la mayor protección posible a los derechos constitucionales afectados por lo que debe ser objeto de interpretación restrictiva, siendo por ello por lo que dice: «*Pero ante la ausencia de esta situación de urgencia no solo frente a la necesaria previa autorización judicial o posibilidad de emisión de una orden de retención y preservación, deberíamos plantearnos seriamente la conveniencia de acoger esta vía menos gravosa y garante de los derechos de las posibles personas afectadas».* Sobre este mismo aspecto ver la Circular de la Fiscalía General del Estado 5/2019, de 6 de marzo, pág. 45.

[390] El deber se secreto profesional es exigido en numerosas profesiones en las que, su mero desempeño conlleva conocer y acceder tanto a hechos como a determinados datos del cliente. Pese a la amplitud con la que este derecho se concibe, el legislador español, en la reforma procesal penal de 2015 acota este secreto solo a los profesionales que se contienen en el art. 416.2 LEcrim, que expresamente dispone que estarán exentos del deber de declarar *«2. El Abogado del procesado respecto a los hechos que éste le hubiese confiado en su calidad de defensor»*. Con esta inclusión expresa dentro del texto legal se determina que sólo están excluidos de la obligación expresa de colaboración dispuesta por la ley, por verse afectado al concurrir un deber de secreto profesional, tan sólo el abogado, con lo que los demás profesionales a los que pudiera afectar la obligación de secreto profesional sí que deberán cumplir con la obligación de colaboración en la retención de datos y su aseguramiento.

[391] Esta obligación, existe también en la diligencia de registro remoto de equipos informáticos, en el art. 588 septies LECrim, y de manera general se impone para las demás diligencias en el art. 588 ter e, LECrim.

acceso a ellos que permitiera destruirlos, ocultarlos, o en cualquier caso, evitar que se pierdan. Se trata de una obligación que se impone para poder ganar el tiempo necesario hasta que se recaba la necesaria autorización judicial para realizar el acceso. Esta volatilidad o fragilidad de los datos almacenados es aún mayor cuando los datos están guardados en la nube, porque la posibilidad de acceder remotamente a ellos desde otro dispositivo distinto, y disponer de su contenido, es mucho más sencilla, y con ello también intensifica el riesgo de una posible pérdida o alteración.

Esta obligación también está contenida en el art. 19.4[392] del Convenio de Budapest y asimismo ya se recogía en el art. 351 del Anteproyecto del Código Procesal penal[393]. Se trata, por lo tanto, de una obligación que ya viene siendo admitida en distintos textos legales.

En cuanto a las características que debe reunir el tercero obligado a acatar esta exigencia, la ley solo dice que será *«cualquier persona que conozca o bien el sistema informático, o bien las medidas aplicadas para proteger los sistemas informáticos contenidos en el mismo»*. No se alude al titular de los derechos de propiedad intelectual o industrial del sistema, con lo que la extensión de la obligación abarca a cualquiera que reúna los conocimientos necesarios para ello.

El obligado es todo aquél que, sin restricción, conozcan los sistemas, personas que, sin ser los titulares del sistema, sepan cómo es su funcionamiento, y más concretamente el modo de acceso y protección de los datos. El contenido de la obligación que se tiene que cumplir también se describe en términos muy genéricos, y consiste en *"facilitar la información que resulte necesaria"*. La persona obligada puede oponerse a la orden recibida en situaciones extremas, que no están descritas por la ley, aunque sólo se alude a la posibilidad de que «*se derive una carga desproporcionada»* de cumplirse con ello. No se ofrecen criterios ni pautas para reconocer esta desproporción[394]. Lo que parece claro es que el acceso sin restricción implica que no se puede pedir a cualquier experto

[392] El precepto dispone que: «*4. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a ordenar a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo que facilite toda la información necesaria, dentro de lo razonable, para permitir la aplicación de las medidas indicadas en los apartados 1 y 2»*.

[393] El art. 351 disponía bajo la rúbrica de *«Deber de colaboración»* que «*1. - Los proveedores de acceso o servicios telemáticos y los titulares o responsables del sistema informático o base de datos objeto del registro están obligado a facilitar a los agentes investigadores la colaboración precisa para la práctica de la medida y el acceso al sistema. Asimismo, están obligados a facilitar la asistencia necesaria para que los datos e información recogidos puedan ser objeto de examen y visualización. 2. - Las autoridades y los agentes encargados de la investigación podrán ordenar a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo que facilite la información que resulte necesaria para el buen fin de la diligencia».*

[394] Los ejemplos de este tipo de desproporción pueden ser muy distintos, sobre todo ante la falta de definición del texto legal, pero pueden ser desde la implicación de derechos económicos del obligado a aportar la información, por ejemplo, la existencia de un acuerdo de no suministra información, otros asociados a la posible afectación a la propiedad industrial o intelectual, etc. En todo caso deberá ser la jurisprudencia la que vaya ofreciendo criterios de dicha desproporción, atendido el hecho, las circunstancias, y el posible derecho afectado por el suministro de la información.

informático que realice estas operaciones de retención, sino a personas que guarden cierta relación directa con la información que se quiere proteger.

La doctrina distingue el contenido de esta obligación y la que se impone por parte del art. 588 septies b LECrim, que más adelante se analizará. Se sostiene que ambas son la misma obligación, y en ambas diligencias de investigación este deber de colaboración debe aplicarse igual[395], aunque el tenor literal en las normas que las regulan no sea idéntico.

4. La diligencia de registro remoto de equipos informáticos.

En el desarrollo de este apartado, se estudiará la segunda de las diligencias que configura el objeto de este trabajo. En una primera aproximación puede decirse de ella que es una diligencia de investigación original por su desarrollo y contenido, y que era una medida de investigación muy esperada. La tecnología, en la actualidad, permite examinar el contenido de un dispositivo mediante aplicaciones que prescinden del artefacto a registrar de forma material, permitiendo literalmente entrar en el mismo para realizar esas tareas de registro, sin necesidad de tener la posesión del dispositivo informático mientras que se practica la diligencia de investigación. Es una diligencia en la que contrasta la sencilla definición que ofrece el texto legal con el modo impreciso e indefinido de llevarse a cabo de modo concreto, evocándose con la lectura del tenor legal el empleo de virus informáticos o medios similares. Es una medida con mucho potencial para la obtención de información, porque abre una ventana directa a cualquier actividad que se realice en el ordenador.

La facilidad con la que a priori se presenta su ejecución, y la amplitud del registro que permite llevar a cabo, es la que justifica que se trate de una diligencia restringida a supuestos muy concretos, de marcada gravedad, y bajos presupuestos de tiempo y forma muy restrictivos.

La redacción del Proyecto de Código Procesal Penal[396] contenía una diligencia de esta naturaleza, con lo que su presencia en la Ley muestra una clara voluntad legislativa de incorporarla al ordenamiento jurídico español. Finalmente, y dada su relación con la posible limitación de los

[395] Vid. RODRÍGUEZ LAINZ, José Luis . «¿Podría un juez español obligar a Apple …..?». Op. Cit. Pág. 6 y 7. El autor esgrime un defecto arrastrado desde las versiones iniciales del Código Procesal Penal hasta la actualidad como explicación a la diferencia, pero estima que son de la misma naturaleza.

[396] El contenido de esta diligencia se encontraba en tres artículos del proyecto de Código Procesal Penal del año 2013, disponible en la web del Ministerio de Justicia en el enlace que a continuación se cita: http://www.mjusticia.gob.es/cs/Satellite/Portal/1292375190463?blobheader=application%2Fpdf&blobheadername1=Content-Disposition&blobheadername2=Medios&blobheadervalue1=attachment%3B+filename%3DCODIGO_PROCESAL_PENAL.pdf&blobheadervalue2=1288778173060. Pág. 171. Se trata de sólo tres artículos, en concreto los artículos 350, 351 y 352, que contrastan en contenido con la actual regulación finalmente aprobada que es mucho más completa y profusa.

derechos contenidos en el art. 18 CE, y muy especialmente el derecho a la intimidad, el derecho al secreto de las comunicaciones, el derecho a la propia imagen, e incluso la posibilidad de que se vea afectado el contenido del derecho al propio entorno virtual tal y como lo estudiamos en otras partes de esta tesis, su regulación completa está en el Capítulo IX del Título VIII.

El modo de ejecución de esta diligencia resulta bastante novedoso y aglutina conceptos tan técnicos como virus informáticos, programas espía, troyanos, y expresiones parecidas, que no son explicados en el texto de la Ley, dejándose por lo tanto a criterio de los investigadores, y al estado de la técnica en cada momento, cómo deba llevarse a cabo su practica en los casos concretos que se vayan sucediendo.

La óptica jurídica conduce a resaltar lo polémico y controvertido que puede llegar a ser esta medida, ante el alto grado de limitación y afectación que provoca su aplicación sobre los derechos del art.18 CE.

El carácter multifuncional de la actividad que se desarrolla con un ordenador es objeto de un completo examen usando esta diligencia, al menos a priori, lo que conlleva poder acceder a datos sobre casi cualquier faceta de la vida del investigado que pasen por este sistema informático. En este sentido, no puede perderse de vista que el uso de un ordenador permite realizar procesos de comunicación, guarda todo tipo de imágenes y de vídeos, documentos tanto personales como profesionales, información sobre transacciones comerciales, guarda las *cookies* del acceso a internet y a las redes sociales, etc. Es evidente que es una ventana abierta a la vida privada del usuario de dicho ordenador y, por ello, debe admitirse de un modo excepcional y muy restringido el examen y registro de esta clase de dispositivos.

La excepcionalidad es, por todo lo anterior, la nota más característica de esta diligencia de investigación, materializándose en aspectos que van desde la clase de datos a obtener, el tiempo de duración de la práctica de la diligencia, los delitos para cuya investigación se puede emplear o la rigurosidad exigida a la resolución judicial habilitante.

Esta diligencia comparte con la de registro de dispositivos de almacenamiento el hecho de que no está pensada para el acceso a las comunicaciones que se desarrollen mediante el empleo de medio tecnológico, pues para eso la Ley cuenta con una diligencia específica[397]. Esta diligencia está creada para poder acceder y registrar los datos que quedan en la memoria del dispositivo empleado por el investigado, y que se generan con su uso habitual, excluyéndose los datos que formen parte de un proceso de transmisión de datos o de comunicaciones vigentes, sin que puedan descartarse las

[397] En concreto el Capítulo III, del Título VIII de la LEcrim sobre "*La detención y apertura de correspondencia escrita y telegráfica*"- arts. 579 a 588 LEcrim; Capítulo V sobre "*La interceptación de las comunicaciones telefónicas y telemáticas*" - arts. 588 ter apartado a hasta art. 588 ter apartado m.

comunicaciones ya producidas. En todo caso, la posibilidad de que las comunicaciones puedan verse afectadas es algo que no cabe ignorar, como expresamente se reconoce en la Circular de la Fiscalía General del Estado 5/2019, de 6 de marzo, al considerar que es una diligencia que está *«a medio camino entre el registro de dispositivos de almacenamiento masivo y la intervención de las comunicaciones»*[398]

Durante la ejecución de este tipo de diligencia no se tiene la disposición efectiva del aparato en el que están todos estos datos, mientras que en la diligencia de los arts. 588 sexies a y siguientes sí. Por eso, para realizar su ejecución se ha de disponer de todos los elementos que permiten localizar dicho aparato, individualizarlo, y acceder a su interior, y con ello a su contenido. La Ley da así carta de naturaleza a un modo de investigación sigiloso y discreto, que minimiza el riesgo de ser descubierto, y asegura la espontaneidad del investigado en todos sus actos, que ante el desconocimiento de la intervención que se está realizando diluye el riesgo de destrucción o alteración de la información buscada[399].

4.1. Delimitación con figuras afines y presupuestos.

El artículo 588 septies apartado a LECrim, bajo la rúbrica de «*presupuestos*», concreta los modos de ejecutar esta diligencia, admitiendo para su realización tan sólo dos formas: en primer lugar, el uso de los datos de identificación y los códigos, como primer método de acceso remoto, y una segunda modalidad sería el acceso al dispositivo informático de forma remota y telemática.

En ambos supuestos se actúa sin el conocimiento del titular o del usuario habitual del equipo, y todo ello se hace mediante «*la instalación de un software»*[400] que lo permita[401].

El legislador opta solo por dos fórmulas sin admitir ninguna otra más, ni prever otros posibles sistemas de acceso en el futuro, lo que refuerza el carácter restrictivo de esta medida que sólo se considera legal en el modo en que se concibe. No caben, por lo tanto, otros métodos de acceso que se ejecuten fuera de los dos legalmente previstos.

---

[398] Circular de la Fiscalía General del Estado 5/2019, de 6 de marzo. Pág. 53.
[399] Vid. ORTIZ PRADILLO, Juan Carlos. *Problemas procesales de la ciberdelincuencia*. Colex. Madrid. 2013. Pág. 191.
[400] Cfr. VELASCO NÚÑEZ, Eloy. Op. Cit. Página 13. El autor alude a wiresharks, arpspoofings, los keyloggers o los softwares troyanos como los ejemplos de esta clase de software que pueden emplear los investigadores.
[401] Vid. RODRÍGUEZ LAINZ, José Luis, «Intervención judicial de comunicaciones vs. registro remoto de equipos informáticos: los puntos de fricción». *Diario la Ley.* Nº 8896, 9 de enero de 2017. LA LEY 10072/2016. Pág. 4. El autor reseña las dos fórmulas de acceso contempladas legalmente.

El artículo no describe el desarrollo y la concreta ejecución de los dos métodos de acceso remoto, con lo que deberemos estar a las prescripciones técnicas de cada momento a los efectos de su practica.

El supuesto que consiste en el registro remoto mediante el empleo de usuario y contraseña parece ser el más simple de los dos descritos, y el que menos problemas presenta en la teoría, con lo que parecerá el más usual.

Por el contrario, el consistente en la instalación de alguna clase de programas espía exige la instalación de dichos programas en el aparato que se desea controlar, lo que exige claramente que se autorice la entrada en el domicilio donde está el ordenador, con la finalidad de instalación del software espía, salvo que haya alguna clase de sistemas que lo hagan innecesario[402]. En todo caso una mayor explicación en cuanto a la forma de instalar este software hubiera sido algo deseable, porque el modo de ejecutar la medida es un aspecto que puede ser impugnado por las defensas. En este sentido, resulta evidente que el modo en que se haya procedido a la ejecución puede depender la validez de la diligencia, porque no olvidemos que el texto legal contempla sólo dos únicos mecanismos de acceso y registro válidos. Por ello, el hecho de que la norma explique poco o nada sobre el desarrollo técnico de la diligencia multiplica las opciones impugnatorias, ya que deja demasiado abierto el modo concreto de ejecución, que deberá explicitarse detalladamente tanto en el oficio policial, como en el auto judicial, para que quede constatada su adecuación a alguna de las dos formas de acceso al dispositivo previstas en el precepto.

En lo que se refiere a la primera de las formas de acceso remoto al ordenador, no se detalla si con las menciones a los conceptos de código o dato de identificación, se está refiriendo a los conocidos "usuario y contraseña" que empleamos todos para entrar en nuestros ordenadores. En todo caso, de ser así, tampoco se explica cómo se han conseguido esos datos de manera previa, y mucho menos si esto hay que ponerlo de manifiesto en el oficio policial, a lo que cabe asentir, pues dicha información debe ser suministrada al Instructor en la medida en que se ha de verificar que estos datos de los que se dispone para poder acceder de modo remoto al ordenador se han conseguido de un modo acorde a la legislación[403]. El segundo sistema de acceso se basa en la instalación de un software especial que permite entrar al contenido del ordenador sin que se indique en el texto legal ningún aspecto técnico sobre el particular.

Sobre esta diligencia alguna doctrina destaca que se caracteriza por mostrar una dimensión estática en el acceso a la información, esto es, está pensada únicamente para el acceso a los datos ya

[402] Circular de la Fiscalía General del Estado 5/2019, de 6 de marzo. Pág. 55 a 57.
[403] El modo de conocer dicho usuario y contraseña puede ir desde que alguien lo haya comunicado a los investigadores o que simplemente estos lo hayan logrado conocer por alguna vía.

contenidos en el equipo informático. Sostiene esta línea de opinión que no se trata de una diligencia configurada para permitir un *«seguimiento de las actividades»*[404] y acumular los datos de interés para la investigación, lo que no habilitaría para el empleo de determinados mecanismos tecnológicos que permiten el rastreo "on line" de todo lo que hace el equipo.

Por el contrario, esta opinión doctrinal parece ser contraria y no encajar con la previsión del art. 588 septies apartado c LECrim, en lo referente a la duración temporal de la medida. Esta norma prevé, al contrario de lo que sostienen estos autores, una intervención dinámica, no estática, sometiendo a la diligencia expresamente a una duración temporal limitada, pero a la que otorga una cierta duración temporal, por breve que sea[405]. El hecho de que para la ejecución de la diligencia se prevea un plazo durante el que podrá desarrollarse, aunque sea un lapso temporal limitado[406], permite avalar el dinamismo ínsito en la medida, lo que además es mucho más acorde con la finalidad de investigación que persigue el legislador.

En suma, lo que esta diligencia permite es que los investigadores puedan conocer cómo se desarrolla una determinada actividad en el tiempo, lo que, lejos de ser algo estático, es todo lo contrario, dinamismo. Por lo demás, este parecer conforme al cual estamos ante una diligencia dinámica también es compartido por la Circular de la Fiscalía General del Estado 5/2019, de 6 de marzo[407].

Una característica importante de esta diligencia es que se trata de una medida concebida para una investigación que haya sido declarada secreta. De hecho, la doctrina la caracteriza como una diligencia apropiada para ser *«practicable en condiciones de discreción y secreto, que tuviera como único objeto, de conformidad con lo establecido en el art. 588 septies a.1 de la LECrim, el descubrimiento de la clave PIN del dispositivo»*[408]. Este aspecto la diferencia de la diligencia de acceso a los dispositivos de almacenamiento masivo de información, que suele ser una diligencia

---

[404] Cfr. OTAMENDI ZOZAYA, Fermín. Op. Cit. Pág. 144. El autor es de esta opinión y utiliza la expresión en el sentido de poner de manifiesto que las dos modalidades de acceso al ordenador limitan sobremanera las posibilidades que ofrece la tecnología actual.

[405] No toda la doctrina observa el dinamismo de la medida del mismo modo. Hay autores que estiman que el acceso a dispositivos de almacenamiento masivo constituye una medida de investigación mucho más estática, y confieren, por el contrario, mucho más dinamismo al acceso remoto a equipos. Vid. RICHARD GONZÁLEZ. Op. Cit. Pág. 15. El autor además también defiende su posible duración prolongada en el tiempo y la posible afectación del derecho a la intimidad y la privacidad del domicilio.

[406] LÓPEZ-BARAJAS PEREA, Inmaculada. «Garantías constitucionales en la investigación tecnológica del delito: previsión legal y calidad de la ley». *Revista de Derecho Político UNED*, Nº 98. enero-abril 2017. Pág. 116.

[407] Pág. 53.

[408] Cfr. RODRÍGUEZ LAINZ, José Luis. «Sobre la naturaleza jurídica de los datos identificadores de aplicaciones de dispositivos de comunicaciones. Comentario a la STS, SALA 2.ª, 551/2016». *Diario La Ley*, Nº 8831, 26 de Septiembre de 2016. LA LEY 6777/2016. Pág. 10. El autor defiende el empleo de esta diligencia de investigación con la mera finalidad de poder acceder al pin de un determinado dispositivo, es decir, como medida puente que permita el empleo de otra diligencia, si bien es verdad que para ello parte de la necesidad de que concurran los requisitos para la adopción de la medida de acceso remoto, lo que restringe su aplicabilidad. Termina defendiendo como vía alternativa recabar de los prestadores de servicios la información necesaria para acceder a un determinado dispositivo.

derivada de una entrada y registro en domicilio, o de la ubicación del dispositivo fuera de uno de ellos. Además, en esta última diligencia, al ser localizado el dispositivo durante el registro, se permite colegir que el afectado estará presente al incautar el dispositivo, lo que le permitirá considerar como algo bastante probable que se solicite el acceso a su contenido. Por el contrario, no parece que esto sea lo que sucede en un registro remoto, donde existe un completo desconocimiento por el investigado de la diligencia que se está llevando a cabo y donde toda la investigación se realiza de manera separada a su conocimiento.

El contenido de las disposiciones legales sobre esta diligencia de registro remoto de equipos informáticos, no limitan su práctica a un sólo ordenador, por lo que puede aplicarse a varios de ellos, y, además, con esta diligencia el objeto de la medida de investigación no se limita o circunscribe al registro de ordenadores, sino que a través de ella puede se puede intervenir cualquier dispositivo electrónico, sistema informático o cualquier instrumento de almacenamiento masivo de información o incluso a una base de datos, y a más de uno de ellos simultánea o sucesivamente, si así se estimara oportuno. Lo que subyace bajo esta enumeración legal es la voluntad del legislador de que la diligencia permita efectuar el registro y la observación de una serie de instrumentos del investigado porque se sospecha que se usan para fines delictivos.

Además, como no puede ser de otro modo, partiendo del concepto amplio de dispositivo que el legislador ha desarrollado, y que ya se analizó en el apartado anterior, con esta diligencia también se permite el registro remoto de la información alojada en la nube. La única diferencia que se aprecia con respecto a la diligencia de registro de dispositivos de almacenamiento, sobre este concreto aspecto, está en el modo de acceso, porque en esta concreta diligencia se hace de modo remoto. No obstante, en todo caso, en cuanto al modo de acceso, habrá de producirse por alguna de las dos modalidades previstas expresamente en la ley como forma de llevarla a cabo, pues cualquiera que no sea alguna de éstas, simplemente no será válida[409].

En esta diligencia, como en la anterior, es extremadamente importante el contenido del auto judicial que la acuerde. Pues, no debe perderse de vista que, en dicho auto, es donde se han de especificar y concretar las razones que han llevado a su adopción, y el mismo deberá cumplir con todos los

[409] La razón que sustenta esta afirmación descansa, por una parte, en el propio tenor de la ley, que es el que determina los modos de acceso que el legislador admite para llevar a cabo un registro remoto de equipos, y, por otro lado, en el hecho de que cualquiera de los sistemas previstos para limitar el contenido de derechos fundamentales tiene que estar previsto por la ley. Si el legislador hubiera admitido otros modos de acceso remoto debería haberlos previsto, pero no parece que éste haya sido el caso, y se ha decantado, exclusivamente sólo por dos métodos que permiten llevarlo a cabo, con independencia de que pudieran existir más ahora, o en el futuro. Esta decisión del legislador, tan limitada, puede comportar un desfase técnico en un futuro cercano, entre el contenido de la norma y la realidad técnica, habida cuenta del progreso que la tecnología va experimentando. Las consecuencias prácticas que esta decisión legislativa representa es una posible inefectividad de la medida y al mismo tiempo la necesidad de actualizar esta concreta norma para que cumpla con la finalidad pretendida, para que se adapte a nuevos medios, más modernos, de acceso remoto.

requisitos necesarios para posibilitar la ejecución de la medida, así como cuantos otros estime necesarios el juez instructor.

En este sentido, dicha resolución autorizando la medida de investigación ha de contener la determinación de cuál de los dos mecanismos de acceso a la información previstos en la norma se van a utilizar en el caso concreto, la descripción acerca del el modo de ejecución elegido, que dependerá de lo que se pida en el oficio policial, y muy especialmente, los aspectos técnicos que se estimen adecuados a los afectos de evitar que se produzca inseguridad jurídica[410], pues de hecho algún sector técnico ha considerado que la ejecución de esta diligencia debería ser llevada a cabo por personal especializado con la titulación específica.

En otro orden de materias, se trata de una diligencia, que, a diferencia de la anterior, se prevé para la investigación de delitos muy concretos y determinados, lo que respeta la pauta seguida por otros ordenamientos jurídicos, y el criterio mantenido en acuerdos internacionales suscritos por España. Se trata de una diligencia de adopción obligada para todos los países que han suscrito el Convenio de Budapest, en los términos que ya explicaron.

En lo referente a su utilización exclusiva para investigar una clase concreta de delitos, esto es, alguno de los incluidos en el listado contenido en el listado contenido en el art. 588 septies a, 1 LECrim [411], se trata de una exigencia que está presente en otros preceptos de la LECrim: art. 579. 1 LECrim, art. 588 ter LECrim o art. 588 quater b) LECrim. En todo caso, se ha de volver a la mención referente a la gravedad del hecho, esto es a la entidad del mismo, o a sus consecuencias penológicas, lo que ha llegado a suscitar sendas interpretaciones doctrinales [412], en orden tanto a

[410] Vid. RUBIO ALAMILLO, Javier. «La informática en la reforma de la Ley de Enjuiciamiento Criminal». *Diario La Ley*, Nº 8662, 10 de Diciembre de 2015, LA LEY 7030/2015. Págs. 9-11. El autor, que es perito informático, alude a la regulación que se ha llevado a cabo en la LEcrim sobre esta materia. Alude a la necesaria preparación técnica que debe tener la persona encargada de analizar el software de acceso al ordenador; critica que en España la ingeniería informática aún no ha sido regulada, pero debería ser una persona con esta capacitación la encargada de llevar cabo el aseguramiento del mecanismo a través del cual esta diligencia debe llevarse a cabo en caso de ser ordenada. El respeto a estas proposiciones le otorga a la medida ejecutada mayores garantías en todos los órdenes implicados: el derivado de la investigación y también del derivado del respeto a los derechos afectados por la medida.

[411] *«a) Delitos cometidos en el seno de organizaciones criminales. b) Delitos de terrorismo. c) Delitos cometidos contra menores o personas con capacidad modificada judicialmente. d) Delitos contra la Constitución, de traición y relativos a la defensa nacional. e) Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación».*

[412] Vid. MIRANDA WALLACE, Dennis. «Registro remoto de equipos informáticos. Comentario crítico al artículo 588 septies LECrim». *Revista General de Derecho Procesal , nº* 42. 2017. Pág. 4. El autor hace mención a un auto dictado por la AP de Tarragona 109/2016, de 6 de abril de 2016 (Sección 4º). Ponente: Don Javier Hernández García. El auto formuló una cuestión prejudicial al TJUE en la que preguntó por la duda interpretativa derivada de la aplicación del art. 579.1 LEcrim, puesto en relación con el art. 588 ter apartado a, de la misma norma legal. El 588 ter, a alude a la necesaria concurrencia de presupuestos exigidos en el art. 579.1 para poder intervenir comunicaciones telefónicas y telemáticas, o que se trate de delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación. La pregunta que se realiza la Audiencia Provincial de Tarragona es si la gravedad del delito como criterio justificador de la interceptación de las comunicaciones sólo puede establecerse en relación con la pena a imponer por el delito, o si además puede tenerse en consideración la conducta

considerar que la gravedad exigida por la ley puede ser entendida en los dos sentidos, esto es, tanto desde el punto de vista de la pena que se puede imponer por el delito conforme al art 13 CP, o bien entendida según el impacto y la alarma social que genera el hecho por sí sólo, prescindiendo de la penalidad que al mismo le pudiera corresponder.

La concreta enumeración de delitos para cuya investigación se puede emplear esta diligencia, está tasada y *«constituyen un numerus clausus»*[413]. La relación de delitos para la que se puede emplear comienza por los tipos penales que son cometidos en el seno de organizaciones criminales[414], lo que

---

delictiva y el nivel de lesividad de en los bienes jurídicos afectados. Además, también pregunta si en todo caso el umbral de gravedad establecido en la pena de tres años de prisión es bastante. Todo ello se pone en relación con el contenido de los arts. 7 y 8 del CDFUE en unión al art. 8 del CEDH. Esta cuestión fue resuelta por la sentencia de la Gran Sala del Tribunal de Justicia de la UE de fecha 2 de octubre de 2018. La sentencia dictada en el asunto C 207/2016 no responde a la cuestión que le fue suscitada, pero aportó un criterio interpretativo, dentro de los considerandos 51 y 53 de la sentencia. Conforme al primero *«el acceso de las autoridades públicas a estos datos constituye una injerencia en el derecho fundamental al respeto de la vida privada, consagrado en el artículo 7 de la Carta, incluso a falta de circunstancias que permitan calificar esta injerencia de «grave» y sin que sea relevante que la información relativa a la vida privada de que se trate tenga o no carácter sensible o que los interesados hayan sufrido o no inconvenientes en razón de tal injerencia. Tal acceso también constituye una injerencia en el derecho fundamental a la protección de los datos personales garantizado por el artículo 8 de la Carta, puesto que constituye un tratamiento de datos personales*», lo que significa que el acceso a datos es una injerencia en un derecho fundamental. El considerando 53 sobre la gravedad viene a decir que *«por lo que se refiere al objetivo de la prevención, investigación, descubrimiento y persecución de delitos, procede observar que el tenor del artículo 15, apartado 1, primera frase, de la Directiva 2002/58 no limita este objetivo a la lucha contra los delitos graves, sino que se refiere a los «delitos» en general»*. En todo caso los considerandos 56 y 57 cierran la cuestión fijando que *« En efecto, conforme al principio de proporcionalidad, en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos solo puede justificar una injerencia grave el objetivo de luchar contra la delincuencia que a su vez esté también calificada de «grave»».* Por su lado el siguiente dice, *«En cambio, cuando la injerencia que implica dicho acceso no es grave, puede estar justificada por el objetivo de prevenir, investigar, descubrir y perseguir «delitos» en general».* Por lo tanto y pese a que no se responde estrictamente a la cuestión que se le planteó, si que se obtiene un criterio de interpretación, conforme al cual cuando la injerencia en los derechos es grave el delito ha de ser también grave. En suma, cuando el art. 579.1 LECrim habla de delitos dolosos castigados con más de 3 años de prisión (también en los 588 ter a) y 588 quáter b), este tipo de delitos no legitimaría el acceso a los datos de tráfico cuando dicha injerencia sea grave porque a tenor del art. 13 CP no son delitos graves, al igual que los cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o de la comunicación o servicio de comunicación del 588 ter a) y 588 septies a) que solamente justificarían una injerencia grave si estuvieran castigados con pena de prisión superior a 5 años.

[413] Cfr. CUCARELLA GALIANA. Luis Andrés. «Autorización judicial de registro remoto de equipos informáticos». *Revista General de Derecho Procesal*, nº 38. año 2016. Pág. 8.

[414] La STS 703/2017, de 25 de Octubre. Ponente: Don Andrés Martínez Arrieta, realiza en su fundamento de derecho noveno un estudio breve, pero suficiente de la nueva regulación de la organización criminal. Creo que es necesario su aportación a los efectos de conocer el parecer de la Sala segunda sobre este particular. Dice la sentencia que: «*De acuerdo a reiterados pronunciamientos de esta Sala, en interpretación del tipo penal de la organización criminal el mismo se conforma como un plus respecto al grupo criminal. Así, en la STS 576/2014, de 18 de julio, dijimos La doctrina de esta Sala (entre las más recientes, Sentencia núm. 426/2014, de 28 de mayo), destaca que la nueva regulación del CP tras la reforma operada por la LO 5/2010, contempla, como figuras delictivas diferenciadas, la organización criminal y el grupo criminal. El art. 570 bis define a la organización criminal como: "La agrupación formada por más de dos personas con carácter estable o por tiempo indefinido que, de manera concertada y coordinada, se reparten diversas tareas o funciones con el fin de cometer delitos, así como de llevar a cabo la perpetración reiterada de faltas".*

Se excluyen, pues, los casos de transitoriedad, antes incluidos en el concepto que aparecía en el art. 369 del Código Penal.

Por su parte el art. 570 ter in fine, describe el grupo criminal como "la unión de más de dos personas que, sin reunir alguna o algunas de las características de la organización criminal definida en el artículo anterior, tenga por finalidad o por objeto la perpetración concertada de delitos o la comisión concertada y reiterada de faltas".

exige estar al contenido de las normas legales que regulan estos tipos delictivos, y la jurisprudencia que los completa.

El empleo de esta diligencia también abarca a la investigación de todos los delitos relacionados con el terrorismo[415]. La definición del texto legal es muy amplia, y se deduce la posibilidad de su aplicación a diversos comportamientos que se pueden enmarcar en el tipo penal de terrorismo. Como ninguno de estos comportamientos es expresamente excluido o diferenciado, hay que interpretar que todos ellos pueden ser objeto de investigación a través de esta diligencia.

Los delitos que se cometan contra menores o personas con capacidad modificada también pueden investigarse empleando esta diligencia. Otra vez se aprecia una alusión genérica acerca de la materia, lo que permitirá emplear esta diligencia para investigar cualquier tipo de delito, fuera el que fuera, y de la gravedad que fuese, siempre que tuviera como sujeto pasivo a personas bajo estas situaciones.

Por lo tanto, la organización y el grupo criminal tienen en común la unión o agrupación de más de dos personas y la finalidad de cometer delitos concertadamente. Pero mientras que la organización criminal requiere, además, la estabilidad o constitución por tiempo indefinido, y que se repartan las tareas o funciones de manera concertada y coordinada (necesariamente ambos requisitos conjuntamente: estabilidad y reparto de tareas), el grupo criminal puede apreciarse cuando no concurra ninguno de estos dos requisitos, o cuando concurra uno solo. De esta forma, se reserva el concepto de organización criminal para aquellos supuestos de mayor complejidad de la estructura organizativa, pues es, precisamente, la estabilidad temporal y la complejidad estructural lo que justifica una mayor sanción en atención al importante incremento en la capacidad de lesión. Por lo tanto, para la apreciación de la organización criminal no basta cualquier estructura distributiva de funciones entre sus miembros, que podría encontrarse naturalmente en cualquier unión o agrupación de varias personas para la comisión de delitos, sino que es preciso apreciar un reparto de responsabilidades y tareas con la suficiente consistencia y rigidez, incluso temporal, para superar las posibilidades delictivas y los consiguientes riesgos para los bienes jurídicos apreciables en los casos de codelincuencia o, incluso, de grupos criminales. .....

La jurisprudencia posterior a la reforma ha esclarecido la diferenciación entre ambas figuras. Entre otras, las STS núm 309/2013, de 1 de abril STS núm 588/2013, de 11 de noviembre, STS núm 950/2013, de 5 de diciembre, STS núm. 1035/2013, de 9 de enero, STS núm. 371/2014, de 7 de mayo o STS núm. 426/2014, de 28 de mayo. En las STS núm. 855/2013 y 950/2013, se recordaba que el legislador, con la reforma pretendía aportar instrumentos útiles:

"1º) Para la lucha contra la delincuencia organizada transnacional, caracterizada por su profesionalización, tecnificación e integración en estructuras legales ya sean económicas, sociales e institucionales, para lo cual se diseña como figura específica la organización criminal, del Art. 570 bis.

2º) Para la pequeña criminalidad organizada de ámbito territorial más limitado y cuyo objetivo es la realización de actividades delictivas de menor entidad, para lo cual se diseña como figura específica el grupo criminal, del Art. 570 ter".

Reconociendo, por lo tanto, dos niveles de peligro para los bienes jurídicos protegidos, que determinan una distinta gravedad en la sanción penal.

En consecuencia, debe evitarse que, influídos por la inercia de la antigua doctrina jurisprudencial referida al viejo art. 369 1 2º CP, se incurra en alguno de los dos errores que comienzan a apreciarse en la jurisprudencia menor: 1º) utilizar una interpretación extensiva del concepto de organización, que conduce a incluir en la organización supuestos más propios, por su gravedad, del grupo criminal. 2º) acudir a una interpretación del concepto de grupo que exija requisitos propios de la organización. En ambos supuestos se corre el riesgo de vaciar de contenido la nueva figura del grupo criminal».

[415] En este caso el elenco de delitos relacionados resulta mucho más amplia, ya que los delitos relacionados con la actuación terrorista abarcan varios preceptos del CP: Adiestramiento y adoctrinamiento (art. 575.1 CP), colaboración a los actos terroristas (art. 577 CP), enaltecimiento (art.578 CP), actividades de propaganda y financiación, etc. Se trata de una modalidad de actividad criminal que recibió una reforma extensa en el año 2010. Para más información Vid. CANO PAÑOS, Miguel Ángel. «Los delitos de terrorismo en el Código penal español tras a reforma de 2010». *La Ley Penal*, Nº 86, Octubre 2011. Pág. 4.

La doctrina se ha percatado de esta falta de concreción en la letra c) del precepto al delimitar el ámbito material de delitos que pueden ser investigados, y por ello se invoca la aplicación del contenido del art. 588 bis a, de la LECrim y de los principios rectores contenidos en el mismo. De manera que, a través de una adecuada aplicación de estos principios se limita la posibilidad de usar una diligencia de gran alcance investigador, y configurada además con una fortísima impronta restrictiva de los derechos fundamentales, para aspectos menores, aunque se enmarquen dentro del tipo penal previsto en el marco de la diligencia[416].

Esta modalidad de investigación también se puede emplear para investigar los delitos cometidos contra la Constitución, los delitos de traición, y los referidos a la defensa nacional. En estos casos la doctrina ha hecho la misma matización que en el caso anterior, pero teniendo presente el hecho de que bajo este epígrafe se recogen en el Código Penal delitos de enorme gravedad junto a otros penados con menor severidad[417]. Por lo cual, en estos supuestos resulta preciso acudir de nuevo a un criterio de ponderación y proporcionalidad, que permita la reflexión serena caso a caso a la hora de acordar la diligencia.

Por último, los delitos cometidos a través de instrumentos informáticos, o de cualquier otra tecnología de la información y la comunicación, son también susceptibles de investigarse mediante esta diligencia. En este caso, como en los anteriormente expuestos, se aprecia en el tenor de la norma una abundancia de expresiones generales a la que debe darse una interpretación que permita una adecuada proporcionalidad en la utilización de esta diligencia, evitando que la misma pueda ser empleada para la investigación de delitos de escasa entidad, aunque sean cometidos empleando las nuevas tecnologías (por ejemplo unos insultos o amenazas leves a través de redes sociales). De modo que también en relación con estos supuestos debe realizarse un sosegado análisis de los hechos que permitan buscar otros medios de investigación menos atentatorios contra los derechos fundamentales que los de esta diligencia cuando se trate de delitos de menor gravedad cometidos a través de instrumentos informáticos o tecnológicos. En consecuencia, en estos casos hay también que ponderar la gravedad y la trascendencia de los hechos para admitir la adopción de esta diligencia de investigación acudiendo a los criterios generales [418].

Por último, cabe destacar que esta diligencia, junto a todas las demás que se contienen en la LECrim, sean o no de investigación electrónica, conforman toda una red de medidas de investigación que pueden estar interconectadas entre sí. Y por ello, no hay razón alguna que impida

[416] MARCHENA GÓMEZ, GONZÁLEZ CUÉLLAR SERRANO. Op. Cit. Pág. 388.
[417] *Idem*, Pág. 389. En este caso, los autores ponen énfasis en la posibilidad de tomar en consideración determinados elementos fácticos del hecho que permitan incluir tipos penales que no encuentran acogida en el tenor literal de la norma positiva.
[418] *Idem*, Pág. 390.

que varias de ellas se empleen en la investigación criminal simultáneamente. La Ley no lo prohíbe expresamente, y afectando a varios derechos del mismo artículo 18 CE, puede resultar conveniente, oportuno, o cuando menos posible, practicar una o varias a la vez si se estima necesario atendidas las circunstancias fácticas que concurran en relación con la comisión del hecho delictivo. Esta compatibilidad en el ejercicio de esta diligencia de investigación con otras diligencias de investigación electrónica explica porqué hay autores que relacionan la ejecución de esta medida con la regulación del llamado "agente encubierto informático" regulado en el art. 282 bis 6 de la LECrim[419].

El agente encubierto es una figura legal que permite, bajo autorización judicial, a los agentes de los Cuerpos y Fuerzas de Seguridad del Estado tener acceso al intercambio de comunicaciones y datos realizados entre personas investigadas, haciéndose pasar por uno de ellos. Esta ocultación autorizada de la personalidad real se realiza con la finalidad de esclarecer la comisión de determinados delitos[420]. Es una medida de investigación pensada para un mayor número de tipos penales que la analizada hasta aquí, que resulta mas limitada y restringida[421]. Pues bien, cabe la posibilidad de que, por vía remota, y mediante el empleo de equipos informáticos se puedan entablar acciones que relacionen al investigado con el agente encubierto, a los efectos de investigar alguna modalidad delictiva admitida. Esto supondría que las resoluciones judiciales que acordasen

[419] El apartado 6 del art. 282 bis en la redacción otorgada por la Ley Orgánica 13/2015, de 5 de octubre dispone que: **"***El juez de instrucción podrá autorizar a funcionarios de la Policía Judicial para actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación con el fin de esclarecer alguno de los delitos a los que se refiere el apartado 4 de este artículo o cualquier delito de los previstos en el artículo 588 ter a.*
El agente encubierto informático, con autorización específica para ello, podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos".

[420] Vid. JIMÉNEZ SEGADO, Carmelo y PUCHOL AIGUABELLA, Marta. «Las medidas de investigación tecnológica limitativas de los derechos a la intimidad, la imagen, el secreto de las comunicaciones y la protección datos». *Diario La Ley*, Nº 8676, Sección Doctrina, 7 de Enero de 2016. Pág. 10. Los autores han señalado esta posibilidad.

[421] Son los enumerados en el párrafo cuarto del art. 282 bis, que son los siguientes: a) Delitos de obtención, tráfico ilícito de órganos humanos y trasplante de los mismos, previstos en el artículo 156 bis del Código Penal. b) Delito de secuestro de personas previsto en los artículos 164 a 166 del Código Penal. c) Delito de trata de seres humanos previsto en el artículo 177 bis del Código Penal. d) Delitos relativos a la prostitución previstos en los artículos 187 a 189 del Código Penal. e) Delitos contra el patrimonio y contra el orden socioeconómico previstos en los artículos 237, 243, 244, 248 y 301 del Código Penal. f) Delitos relativos a la propiedad intelectual e industrial previstos en los artículos 270 a 277 del Código Penal. g) Delitos contra los derechos de los trabajadores previstos en los artículos 312 y 313 del Código Penal. h) Delitos contra los derechos de los ciudadanos extranjeros previstos en el artículo 318 bis del Código Penal. i) Delitos de tráfico de especies de flora o fauna amenazada previstos en los artículos 332 y 334 del Código Penal. j) Delito de tráfico de material nuclear y radiactivo previsto en el artículo 345 del Código Penal. k) Delitos contra la salud pública previstos en los artículos 368 a 373 del Código Penal. l) Delitos de falsificación de moneda, previsto en el artículo 386 del Código Penal, y de falsificación de tarjetas de crédito o débito o cheques de viaje, previsto en el artículo 399 bis del Código Penal. m) Delito de tráfico y depósito de armas, municiones o explosivos previsto en los artículos 566 a 568 del Código Penal. n) Delitos de terrorismo previstos en los artículos 572 a 578 del Código Penal. o) Delitos contra el patrimonio histórico previstos en el artículo 2.1.e de la Ley Orgánica 12/1995, de 12 de diciembre, de represión del contrabando. Además, deben sumarse los contemplados en el art. 588 ter a de la LECrim, que como es conocido, es un precepto que lo que hace es efectuar una remisión al art. 579.1 de la misma norma legal, con lo que se amplia el listado de delitos susceptibles de ser investigados mediante el agente encubierto informático a los mismos tipos penales que pueden dar lugar al acuerdo de la intervención de comunicaciones telefónicas y telemáticas.

la realización de cada una de estas diligencias, se dictasen de manera que, de forma interrelacionada, valorasen los presupuestos de ambas.

Finalmente hay que señalar que el registro remoto de equipos es una diligencia sobre la que el Tribunal Supremo no ha tenido la oportunidad de pronunciarse, y tampoco abundan las resoluciones de juzgados y Tribunales de primera instancia sobre ella. De hecho, básicamente sólo se pueden encontrar algunos autos que resuelven recursos de apelación sobre la oportunidad de la medida, pero sin que exista un estudio en profundidad que valore y analice el concreto modo de llevar a efecto esta diligencia en los casos concretos en los que se haya utilizado[422].

4.2. Requisitos generales y específicos para acordar la diligencia.

Las diligencias de investigación electrónica están sometidas al cumplimiento de una serie de requisitos. Algunos de ellos tienen un alcance general, que afectan a todas las diligencias, sin excepción; por el contrario, otras diligencias requieren, además del insoslayable respeto a los principios generales, la concurrencia de unos requisitos específicos. En el caso de la diligencia de registro remoto de dispositivos, dado su potencial de afectación y restricción de los derechos fundamentales, deberán respetarse los presupuestos y requisitos propios de la limitación de los derechos del art. 18 CE. Esto implica que deba dictarse un auto que autorice la limitación o restricción de alguno de esos derechos que pueda verse afectado, que razonará y valorará los principios generales aplicables a todas las diligencias de investigación tecnológica (art. 588 bis a LECrim), así como las circunstancias del hecho. Además de las medidas generales, en el caso concreto de esta diligencia de investigación, ha de respetarse el contenido del párrafo segundo del art. 588 septies a LECrim.

La resolución judicial, por lo tanto, deberá repasar expresamente la concurrencia en los hechos descritos de los principios de proporcionalidad, necesariedad, idoneidad, excepcionalidad y especialidad. Para ello comprobará que la investigación llevada a cabo, así como los indicios encontrados, apuntan a la comisión de alguno de los tipos penales específicos que pueden ser investigados mediante la adopción de la diligencia de registro remoto de equipos electrónicos. En este sentido, lo que procede es llevar a cabo, a priori, un somero análisis en el que se determine si

[422] A los efectos de tener constancia de la ausencia de aplicación que hasta el momento ha tenido esta diligencia debemos recoger una noticia del diario EL PAIS en la que se hace alusión a la primera operación policial en la que se ha usado la figura. MANRIQUE C. SÁNCHEZ. *La Guardia Civil introduce un infiltrado en una red internacional de pederastas por WhatsApp.* Alicante 17 enero 2018 - 13:56 CET. Diario El País. Puede consultarse en https://politica.elpais.com/politica/2018/01/17/actualidad/1516189504_379017.html-

concurren los presupuestos específicos y propios de esta diligencia de investigación electrónica, para posteriormente, si ello es así, realizar un análisis exhaustivo tanto de los presupuestos generales, que son necesarios en todo caso, como de los exclusivos de esta diligencia, pues carecería de todo efecto práctico realizar una valoración acerca de la existencia de los presupuestos o principios comunes, si no concurren, de entrada, los presupuestos específicos.

La aplicación del principio de especialidad es muy importante en relación con esta diligencia porque no basta con seguir la investigación sobre hechos concretos que revistan el carácter de delito, sino que debe tratarse de un delito muy determinado. No puede utilizarse la intervención remota de equipos para investigar cualquier clase de delito, como lo permitiría el art. 588 bis apartado a, 2 LECrim y la jurisprudencia constitucional[423], sino que deberá ser un tipo de los que describe el art. 588 septies, apartado a, párrafo primero LECrim.

Estas tipologías penales admiten cierta amplitud en su conceptuación, porque el art. 588 septies, a, no detalla cada tipo penal en concreto, sino que recoge una categoría genérica, permitiendo incluso acudir a la realización de diversos tipos penales cubiertos por estas modalidades comisivas.

Es decir, aunque se trate de una diligencia de investigación cuyo empleo ha de ser restrictivo, se admite la posibilidad de que se utilice para investigar la concreta comisión de cada una de las diferentes modalidades comisivas que se admitan dentro del tipo penal que admita ser investigado empleando esta diligencia de investigación electrónica. En todo caso es conveniente valorar estos aspectos durante la ponderación y aplicación de los principios generales, conforme la doctrina ha ido reseñando, tal y como se ha visto.

El principio de proporcionalidad también resulta aplicable a esta diligencia. Como es bien sabido, el Tribunal Constitucional[424] ha señalado, que se trata de un principio que permite comparar el

[423] A efectos de citar un ejemplo, se pone en valor las palabras de la STC 104/2006, de 3 de abril. Ponente: Doña Emilia Casas Bahamonde. En dicha sentencia, donde se analizan muchos de los requisitos que a nivel de principios rectores de toda intervención han alcanzado el rango de norma legal, se dice sobre el principio de especialidad que: «l*os elementos necesarios para ponderar que la medida se ajusta al principio de proporcionalidad y que se ha acordado, no como medida prospectiva genérica para la investigación delictiva, sino en relación con personas y hechos delictivos determinados, respecto de concretas líneas telefónicas con sujeción a plazos prefijados. De forma que las resoluciones judiciales de autorización de las intervenciones telefónicas deben contener datos relativos al marco espacial –líneas telefónicas delimitadas–, temporal –plazos–, objetivo –hechos delictivos investigados– y subjetivo –personas conectadas con los hechos delictivos y titulares o usuarios de las líneas telefónicas– de la misma, y la ejecución policial de la medida debe efectuarse en el marco fijado en las autorizaciones judiciales».*

[424] STC 82/2002, de 22 de abril. Ponente: Doña Emilia Casas Bahamonde. La sentencia expresamente alude y explica este principio con las siguientes palabras «*principio de proporcionalidad; es decir, cuando su autorización se dirige a alcanzar un fin constitucionalmente legítimo, como acontece en los casos en que se adopta para la prevención y represión de delitos calificables de infracciones punibles graves y es idónea e imprescindible para la investigación de los mismos (SSTC 49/1999, de 5 de abril, F. 8;166/1999, de 27 de septiembre, FF. 1 y 2; 171/1999, de 27 de septiembre, F. 5; 126/2000, de 16 de mayo, F. 2; 299/2000, de 11 de diciembre , F. 2; 14/2001, de 29 de enero, F. 2; y 202/2001, de 15 de octubre, F. 2; entre las últimas); de modo que la comprobación de la proporcionalidad de la medida ha de efectuarse analizando las circunstancias concurrentes en el momento de su adopción (SSTC 126/2000, de 16 de mayo, F. 8; y 299/2000, de 11 de diciembre, F. 2)2…….El presupuesto habilitante es, como hemos afirmado*

derecho que se afecta o restringe con la finalidad perseguida con la diligencia de investigación que se pretende adoptar. Ya se vio que los criterios comparativos son muy diversos y amparan diversas circunstancias como: perseguir delitos graves, evitar peligros para las personas y el Estado, etc. Sin embargo, parece que la aplicación del principio de proporcionalidad a esta concreta diligencia ha sido ya realizada por el legislador, al concretar y determinar qué tipos de delitos se pueden investigar mediante su empleo, eliminando el resto de delitos por graves que pudiera parecer. El legislador ha preferido limitar su uso para investigar aquellos delitos que muestren un grado de lesividad, gravedad y urgencia suficientes. Fuera de estos supuestos concretos previstos expresamente en la norma, por más determinados, graves y lesivos que pudieran parecer los hechos objeto de investigación, desde un punto de vista social, no podrá acordarse la medida de intervención remota de equipos.

Lo dicho con respecto a la proporcionalidad, también puede apreciarse con respecto al principio de especialidad, esto es, la existencia de un reforzamiento de este principio dentro del propio texto legal. Ello se constata en tanto que el tenor literal de la ley exige la concurrencia de determinados presupuestos penales sustantivos para que proceda la adopción de esta diligencia de registro remoto de dispositivos. El reforzamiento dentro del propio texto legal del principio de especialidad, como ocurriera como con el principio de proporcionalidad, también acontece en alguna otra diligencia que exige su aplicación para investigar tipos penales concretos[425].

El principio de necesidad exige expresar las razones que hacen de la medida solicitada la única posible para poder investigar los hechos, y obtener una determinada información, por consiguiente, debe detallarse suficientemente todo cuanto exprese dicha exigencia y funde su necesaria utilización en la investigación. Por tanto, se debe acreditar que no hay alternativa menos lesiva para obtener la información necesaria sin lesionar el derecho fundamental afectado.

La necesidad puede derivarse de circunstancias que deben valorarse en el auto que resuelva sobre esta diligencia. A título enunciativo, factores como: el tiempo, la emergencia de los hechos, la alarma social, la inexistencia de otros métodos menos invasivos para los derechos fundamentales, que permitan poder culminar rápidamente la investigación cuando sea necesario, o bien la necesidad

---

reiteradamente, un «prius» lógico «pues, de una parte, mal puede estimarse realizado ese juicio, en el momento de adopción de la medida, si no se manifiesta, al menos, que concurre efectivamente el presupuesto que la legitima. Y, de otra, sólo a través de esa expresión podrá comprobarse ulteriormente la idoneidad y necesidad (en definitiva, la razonabilidad) de la medida limitativa del derecho fundamental». Son numerosas las sentencias del mismo TC que se pronuncian en los mismos términos, dejando también citada la STC 202/2001, de 15 de octubre. Ponente: Don Guillermo Jiménez Sánchez.

[425] Otras diligencias de investigación que sólo pueden utilizarse para investigar delitos muy determinados son la diligencia de detención y apertura de correspondencia escrita prevista en el art. 579.1 apartados 1º a 3º, y en la interceptación de las comunicaciones telefónicas y telemáticas que se regulan en el art. 588 ter, apartado a), por remisión; también es exigido un requisito similar en la diligencia de captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, concretando tal exigencia en el art. 588 quáter apartado b.

de continuar con la misma[426], pueden justificar la concurrencia del principio de necesidad en su adopción[427].

El principio de idoneidad también ha de ser valorado para autorizar la práctica de esta diligencia. La idoneidad se define como la cualidad que tiene la diligencia de investigación para alcanzar el objetivo pretendido, y por ello, se ha de analizar si la intervención remota de un dispositivo servirá para recabar algún dato concreto y fundamental, que contribuya a esclarecer los hechos, tales como imágenes, datos sobre una operación económica en tiempo real, un acceso a la red para hacer una transferencia de archivos, o cualquier otro indicio que en forma de dato informático acredite la perpetración del hecho investigado[428].

En lo que se refiere al principio de excepcionalidad, como principio relacionado con el de idoneidad, ha de apreciarse bajo el prisma de que sólo mediante el empleo de la diligencia se pueda conseguir información para la investigación. Ha de acreditarse que el registro remoto es la medida insustituible para obtener datos que permitan avanzar en la investigación emprendida, y que sin llevarla a cabo no se conseguirá culminarla. Además, debe ser la medida que no puede sustituirse por otra distinta, y menos gravosa para los derechos fundamentales implicados[429].

En suma, se trata de justificar ante el Juez Instructor que la grave invasión de los derechos en juego, que supone la práctica de esta diligencia, se verá compensada con el beneficio colectivo

---

[426] STC 115/2013, de 9 de mayo. Ponente: Don Manuel Aragón Reyes. En dicha sentencia se pone un especial énfasis en el factor temporal y de urgencia derivada de los hechos a los efectos de justificar la concurrencia del principio de necesidad. Del tenor literal de la resolución puede leerse «*En tercer lugar, si bien los agentes de policía accedieron a los datos recogidos en la agenda de contactos telefónicos del terminal móvil del recurrente sin autorización judicial (ni tampoco consentimiento del afectado), ya hemos adelantado que tal exigencia se excepciona en los supuestos en que existan razones de necesidad de intervención policial inmediata para la averiguación del delito, el descubrimiento de los delincuentes o la obtención de pruebas incriminatorias, siempre que se respete el principio de proporcionalidad (SSTC 70/2010, FJ 10, y 173/2011, FJ 2, entre otras), como acontece en el presente caso, conforme pasamos seguidamente a exponer.*
….. en el presente caso el acceso policial a la agenda de contactos de los teléfonos móviles que encontraron encendidos en el lugar de los hechos constituye una diligencia urgente y necesaria para tratar de averiguar la identidad de alguna de las personas que huyeron cuando fueron sorprendidas, in fraganti, custodiando un importante alijo de droga, evitando así que pudieran sustraerse definitivamente a la acción de la Justicia. Concurrían, pues, ex ante las razones de urgencia y necesidad que legitiman constitucionalmente la intervención policial conforme a nuestra doctrina (STC 70/2002, FJ 10). Razones de urgencia y necesidad que, en este caso, vienen además avaladas por la flagrancia del delito, circunstancia que refuerza la necesidad de intervención inmediata de la Policía Nacional». En alguna otra ocasión el TC ha considerado que se ve justificada la necesidad con el mero hecho de resultar imprescindible continuar con la investigación STC 82/2002, de 22 de abril. Ponente: Doña María Emilia Casas Bahamonde.

[427] Por tomar un ejemplo que ilustre la aplicación del principio de necesidad imaginemos el supuesto de una persona privada de libertad. Los agentes investigadores pueden tener razones para pensar que el sospechoso utiliza un ordenador portátil para guardar fotografías del secuestrado, o del lugar de los hechos, o bien haya mantenido alguna clase de seguimiento de ésta, o puede haber remitido alguna comunicación, guarde alguna localización mediante el GPS que el dispositivo incorpora, etc. Todos estos elementos, unido al factor tiempo, pueden contribuir a que se considere la medida como necesaria.

[428] STC 56/2003, de 24 de marzo. Ponente: Doña Elisa Pérez Vera.

[429] STC 72/2010, de 18 de octubre. Ponente: Don Eugenio Gay Montalvo.

conseguido, al desvelar aspectos de la investigación criminal que sin su realización resultarían prácticamente imposibles de obtener.

Pero, tal y como se ha dicho, no sólo basta con realizar una exposición de la concurrencia de los principios rectores generales, así como de los demás criterios de aplicación común a todas las diligencias, sino que además, han de concurrir, para poder adoptar una diligencia de registro remoto de equipos informáticos, los presupuestos específicos para su adopción que se recogen en el párrafo segundo del artículo 588 septies, a) LECrim.

En consecuencia, la diligencia de registro remoto deberá ser autorizada por una resolución judicial que debe tener un contenido mínimo obligado. El tono de exigencia respecto de este contenido deriva directamente del texto legal cuando indica que *"deberá especificar"* estos elementos.

Por el contrario, quiénes vayan a solicitar la práctica de esta diligencia, deberán dar al instructor todos los datos necesarios para que la resolución judicial no adolezca de la falta del contenido legal imprescindible, estimándose que la omisión de los datos necesarios debe abocar a la denegación de la diligencia interesada, sobre todo si, una vez requerido el complemento de esa información, no se aporta en un oficio complementario de la solicitud inicial de la diligencia.

La resolución judicial ha de indicar los dispositivos o sistemas objeto de la medida de investigación. El art. 588 septies a) LECrim menciona los dispositivos a los que puede serle aplicable esta medida, pero el apartado 2, letra a), aunque coincide, en lo sustancial, con la enumeración aludida más arriba (ordenadores y dispositivos electrónicos en general), introduce algunas categorías distintas que sólo se encuentran en el enunciado de este precepto: *"sistemas informáticos o parte de los mismos"*, "*medios informáticos de almacenamiento de datos o bases de datos, datos u otros contenidos digitales"*. Esta amplitud descriptiva permite incluir entre los dispositivos sobre los que puede aplicarse la diligencia de registro remoto, a los sistemas de archivo virtuales cuyo acceso se realiza mediante el ordenador que se interviene, en tanto que en dichos sistemas puede alojarse información a la que se puede acceder cuando se emplea el ordenador intervenido.

Las consideraciones realizadas en los párrafos anteriores han de completarse con lo ya analizado en el estudio de la diligencia de acceso a dispositivos de almacenamiento masivo de información, sobre los repositorios de datos y la alocución "sistema informático". El legislador ha realizado un diseño omnicomprensivo de situaciones que, a su juicio, podrían justificar el empleo de esta diligencia. Por lo tanto, si el tenor legal de la diligencia de registro remoto, admite que se pueda obtener la información buscada registrando "*medios informáticos de almacenamiento de datos o bases de datos, datos u otros contenidos digitales",* resulta claro que el legislador lo que ha pretendido es que el examen interno del ordenador no se ciña a los datos colocados en determinadas ubicaciones internas del dispositivo, sino que se pretende encontrarlos donde sea que estén

ubicados, incluso aunque estén fuera del ordenador. Esta es, por consiguiente, una diligencia que admite ejecutarse tanto sobre un dispositivo físico, como lo es el ordenador, como en uno virtual, como lo es la nube a la cual se accede usando el ordenador intervenido.

Hay que volver a reiterar algo que ya se ha dicho desde la introducción de este trabajo, y es que para las dos diligencias de acceso y registro de datos, el auténtico objeto de investigación lo configuran los datos asociados al comportamiento criminal del investigado, aspecto que viene siendo destacado por la doctrina cuando dice que *«un concepto tan etéreo, abstracto, como es la identidad que perfila el objeto instrumental de una injerencia sobre comunicaciones, se convierte en algo físico, tangible aunque sea de forma virtual, en el art. 588 septies a.2,a)»*[430].

La comparación de la regulación de ambas diligencias permite apreciar cierto paralelismo en este aspecto de su ordenación, aunque, sin duda, no exista plena identidad. A diferencia de lo establecido en el art. 588 sexies c, apartado 3 LECrim, conforme al cual el acceso al contenido virtual era posible siempre que *"los datos sean lícitamente accesibles por medio del sistema inicial o estén disponibles para éste"*, no hay una disposición textualmente equivalente en la regulación de la diligencia de registro remoto.

No se conocen las razones por las que el legislador no ha equiparado ambas diligencias en este punto, y las explicaciones que se ofrecen van desde un olvido involuntario hasta el entendimiento del ordenador como un "portal de acceso" a los datos virtuales. Por eso conforme a esta segunda idea se mantiene por la doctrina que *«el legislador ha descartado el conflicto en este punto, asumiendo simplemente que lo que puede verse en España está en España»*[431]. Son asumibles también, opciones que pasan por negar el acceso a redes virtuales, por su implicación con cuestiones de competencia territorial y por la extralimitación con respecto al Convenio de Ciberdelincuencia.

El contenido mínimo de la resolución también debe comprender el alcance de la intervención, el modo en que se producirá el acceso al dispositivo, y la forma en que serán aprehendidos los datos.

---

[430] Cfr. RODRÍGUEZ LAINZ, José Luis. «Intervención judicial de comunicaciones vs…. ». Op. Cit. Pág. 7.

[431] Cfr. VALVERDE MEGÍAS, Roberto. *Intervención de comunicaciones telemáticas y registro remoto*. Ponencia realizada en los cursos de formación continuada realizados en fecha 27 de abril de 2016 bajo la denominación de "La interceptación de las comunicaciones telefónicas y telemáticas". Pág. 30 y 31. Puede consultarse en: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20Valverde%20Meg%C3%ADas,%20Roberto.pdf?idFile=c740b0e1-8842-4ef7-8983-23c4a0732291. Este autor es consciente de los problemas que se derivan de la ubicación virtual de los datos, y cómo este asunto se complica con cuestiones de jurisdicción y competencia. En este sentido, el autor recuerda que fue una cuestión que suscitó cierta polémica durante el desarrollo del proyecto de Código Procesal Penal, pero que allí quedó resuelta. Advierte que es posible que el legislador haya partido de la consideración de que toda información que pudiera ser visitada o visionada desde el interior del territorio nacional, es equivalente a su efectiva radicación en el mismo, y que por consiguiente no resulta necesaria mayor apreciación sobre el particular. Es una de las interpretaciones expuestas en esta materia.

También debe pronunciarse expresamente sobre el software que se empleará para el acceso al ordenador[432] y qué agentes se encargarán de ejecutar la medida.

Los apartados d) y e) del 588 septies a), 2 LECrim, requieren, además, un pronunciamiento acerca del modo en que se realizarán y conservarán copias de los datos obtenidos, y sobre las concretas medidas que se adoptarán para asegurar la integridad y preservación de los datos que se obtengan. Se trata de una disposición muy similar a la del art. 588 sexies, apartado c. 1) LECrim, relativa al registro de dispositivos de almacenamiento masivo de información., que ya se analizó.

La regulación que contiene la LECrim, en los dos casos, exige que la resolución judicial que concrete qué datos son el objeto de búsqueda, entendido esto como qué clase de archivos se buscan, de qué fecha pueden ser, de qué modo se realizara la copia, si debe o no estar presente el Letrado de la Administración de Justicia cuando se extraigan los datos, o si va a estar presente durante la practica de estas acciones, a efectos de otorgar mayores garantías de transparencia, el investigado o su letrado. La norma, sobre estos aspectos, ofrece tanto criterios de búsqueda de información, como formas de ejecución y conservación[433]. También abre la puerta a que sea el Juez Instructor el que fije el modo en que se ha realizar la diligencia, de modo que se practique de la forma más ajustada a las necesidades de la investigación, haciéndola compatible con los derechos afectados por la misma y con los demás derechos procesales del investigado. La Ley, lejos de cerrar todo cuanto se refiere a su práctica, confiere libertad para configurarla a medida de los hechos que se investigan.

En el desarrollo del contenido mínimo, que debe tener el auto que acuerde el registro remoto, el art. 588 septies, apartado e, LECrim, exige un pronunciamiento acerca de la posible supresión de los datos que se encuentren en el interior del dispositivo intervenido. Al ser una medida que arrebata al usuario los datos que estaba empleando, se ofrece por parte del legislador una alternativa de carácter técnico a esta supresión, que es la de evitar un nuevo acceso a los mismos, sin que tenga que llegarse a la eliminación. Entra dentro de lo probable que de producirse la supresión de los datos el usuario pudiera sospechar que se está llevando a cabo una posible investigación, y que tome conocimiento de ella, lo que podría hacer peligrar las pesquisas emprendidas.

Junto a todo lo anteriormente descrito, el apartado c) del art. 588 septies a) LECrim también requiere que se concrete quienes serán los agentes autorizados judicialmente para la ejecución de la medida de investigación. El tenor legal se refiere a los agentes, y no dice cuerpo de seguridad del

[432] Sobre este aspecto ver Pág. 60 de la Circular de la Fiscalía General del Estado 5/2019, de 6 de marzo, que advierte del contenido de la Ley 9/1968, de 5 de abril, de secretos oficiales, relacionado con el Acuerdo de Consejo de Ministros de 6 de junio de 2014. La conjunción de ambas normas permitiría a los investigadores no informar sobre el concreto método de acceso al ordenador, ya que muchas de las técnicas empleadas no pueden ser desveladas.

[433] Por ejemplo, permite que se busquen tan sólo imágenes, si se trata de una célula terrorista que incita a la yihad, o audios en los casos en los que se investigue algún delito en el que se tienen indicios de que hay alguna fuente de prueba de esa naturaleza.

Estado o división orgánica dentro de cada uno de esos cuerpos. El artículo exige expresamente que se indiquen quiénes serán *"los agentes autorizados"* para realizar esta diligencia. Estamos ante una precisión que no suele ser frecuente en la práctica habitual de otras diligencias de investigación, como, por ejemplo, en la de registro de dispositivos o intervenciones de comunicaciones, en la que lo frecuente es designar sólo el cuerpo o unidad policial que estará encargado de llevarlo a cabo. Se trata de una novedad en la Ley actual, que es comprensible, en la medida en que otorga mayor seguridad jurídica, a la hora de poder conocer qué titulación, conocimientos o especialidad puede reunir el agente encargado para realizar la diligencia. En todo caso, dado que el Juez puede exigir cualquier complemento al oficio para que se dote de mayor garantía a la medida, podría requerir que los agentes encargados de realizar esta diligencia reuniesen los conocimientos técnicos necesarios para llevarla a cabo.

En otro orden de cuestiones, es fácilmente constatable que el tenor del art. 588 septies a LECrim, párrafo tercero, es parecido al del art. 588 sexies c, apartado 3 de la LECrim[434]. El apartado tercero permite extender la diligencia inicial de registro remoto de un equipo informático a otros sistemas informáticos o partes del mismo, para lo cual es necesario que se ponga este extremo en conocimiento del Juez Instructor a los efectos de que conceda o deniegue la ampliación que pudiera solicitarse.

Se trata de una ampliación de registro hipotética, similar a la que se vio al analizar el contenido del art. 588 sexies, apartado c, párrafo tercero LECrim, aunque no es completamente idéntica. La comparativa entre los dos artículos permite apreciar que mientras en el art. 588 sexies, apartado c, párrafo tercero LECrim se permite que, por razones de urgencia, el acceso al dispositivo se realice de manera inmediata siendo ello ordenado por la policía judicial o por el Ministerio Fiscal, esto no sea posible en la diligencia de registro remoto de equipos informáticos.

Por lo tanto, cualquier ampliación del registro remoto de un equipo informático debe ser objeto de una resolución separada, cuando con ello se pretenda abarcar "*otros sistema informático o parte de*

[434] «*3. Cuando quienes lleven a cabo el registro o tengan acceso al sistema de información o a una parte del mismo conforme a lo dispuesto en este capítulo, tengan razones fundadas para considerar que los datos buscados están almacenados en otro sistema informático o en una parte de él, podrán ampliar el registro, siempre que los datos sean lícitamente accesibles por medio del sistema inicial o estén disponibles para este. Esta ampliación del registro deberá ser autorizada por el juez, salvo que ya lo hubiera sido en la autorización inicial. En caso de urgencia, la Policía Judicial o el fiscal podrán llevarlo a cabo, informando al juez inmediatamente, y en todo caso dentro del plazo máximo de veinticuatro horas, de la actuación realizada, la forma en que se ha efectuado y su resultado. El juez competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de setenta y dos horas desde que fue ordenada la interceptación».*

este", garantizándose una valoración individualizada por parte del Juez instructor[435]. En la práctica, esto implicará la presentación de una nueva solicitud relativa a la ampliación.

En definitiva, cabe decir, que la diligencia de registro remoto se convierte en una diligencia de potente alcance invasivo en la esfera de los derechos fundamentales, y que, en consecuencia, presenta numerosos requisitos y exigencias, que hacen que su adopción se muestre compleja tanto por razones técnicas, como jurídicas.

4.3. La presencia de terceros: el deber de colaboración y la afectación de la diligencia. Aplicación temporal de la medida.

Las dos diligencias de registro de dispositivos, tanto en su modalidad presencial como en la virtual, han regulado un conjunto de obligaciones que le son exigibles a los que, reuniendo los conocimientos técnicos necesarios, puede coadyuvar a una mejor y más rápida investigación.

En lo que se refiere a la diligencia de registro remoto de equipos informáticos, el art. 588 septies, apartado b LECrim, distribuye en cuatro párrafos, bajo la denominación de *"deber de colaboración",* la regulación del auxilio que los agentes investigadores pueden recabar de terceras personas. Se trata de sujetos obligados a prestar su colaboración a los investigadores, porque tienen conocimientos técnicos específicos acerca del sistema informático al que se ha de acceder, registrar y observar en el tiempo concedido para ello.

Se trata de una imposición que va asociada a los conocimientos que el sujeto obligado tiene acerca del programa o dispositivo al que se pretende acceder y posteriormente registrar, y que, siendo aplicados a estas labores de acceso y de registro, lo posibilitan. Es, por lo tanto, una obligación que, en buena parte de los casos, irá dirigida a personal con conocimientos técnicos e informáticos aplicados al dispositivo a registrar, con lo que tanto las personas encargadas de mantener estos equipos o de administrar tales sistemas informáticos serán los principalmente afectados por estas obligaciones, pero tampoco quedan excluidos los programadores de dichos sistemas, y en general, cualquier persona que pueda interactuar con tales dispositivos y artefactos. El legislador no ha ceñido la obligación a ninguna persona concreta, con lo que cualquiera que reúna un conocimiento efectivo del sistema a registrar puede verse afectado por aquella.

[435] Vid. OTAMENDI ZOZAYA, Fermín. *Las últimas reformas de la Ley de Enjuiciamiento Criminal. Una visión práctica tras un año de vigencia*. Dykinson. Madrid. 2017. Pág. 146.

Es una obligación muy similar a la que existe en la diligencia de registro de dispositivos, si bien la diferencia en este caso reside en el modo de acceso a estos, que están en el interior de un ordenador que sigue siendo empleado por el investigado, o por terceros. En todo caso el contenido de esta obligación, comparada con la del art. 588 sexies, apartado c, párrafo, 5 LECrim, es muy semejante y obliga a los mismos sujetos en los mismos términos en ambos casos[436].

La hipotética necesidad de auxilio en el trascurso de estas dos diligencias se deriva de la utilidad que tiene aprovechar el conocimiento interno de los sistemas operativos que reúnen las personas que usan estos dispositivos, o la ubicación de los datos en el servidor de una empresa, o en un servidor privado, si bien, apunta la doctrina, que debe ser una obligación que se exija con cierta cautela[437].

El párrafo primero del art. 588 septies b, LECrim incluye, entre los obligados a prestar esta ayuda, a sujetos entre los que incluye a *"prestadores de servicios"*, *"personas señaladas en el art. 588 ter apartado e)"*, o *"titulares y responsables del sistema informático o base de datos"*. La relación tan abierta de personas obligadas abarca, desde el titular del aparato, hasta el que tiene conocimientos técnicos sobre el funcionamiento del sistema o del dispositivo. Entre los obligados no están los fabricantes de los equipos, ausencia que puede obstaculizar el acceso a la información que persigue esta diligencia de investigación[438]. La razón de su falta de inclusión puede estar la tutela de la propiedad intelectual. En todo caso, los obligados han de prestar una colaboración activa que

[436] Cfr. RODRÍGUEZ LAINZ, José Luis. «Tres cuestiones polémicas sobre el registro de dispositivos electrónicos de almacenamiento masivo de información». *Base doctrinal Ed. Sepín*. nº documento sp/doct/21066. Septiembre 2016. Pág. 8. El autor además de apoyar la idea del tratamiento unitario de estas obligaciones arroja un argumento más tendente a apoyar su exégesis, aplicando el contenido de la Ley 9/2014, de 9 de mayo, Ley General de Telecomunicaciones. Dicha norma consagra en su art. 39 el deber de los operadores de comunicaciones de garantizar el derecho al secreto de las comunicaciones, con las excepciones que se van desgranando en los once apartados en que se divide el artículo. El autor recurre al contenido del apartado 11 que dispone que "«*En el caso de que los sujetos obligados apliquen a las comunicaciones objeto de interceptación legal algún procedimiento de compresión, cifrado, digitalización o cualquier otro tipo de codificación, deberán entregar aquellas desprovistas de los efectos de tales procedimientos, siempre que sean reversibles».* Acude igualmente al contenido del art. 42 de la misma norma legal que establece la obligación de ceder los datos de procesos comunicativos cuando se trate de la investigación de delitos graves.

[437] BUENO DE MATA, Federico «Comentarios críticos y reflexiones acerca de las últimas reformas procesales en materia de investigación tecnológica» en RODRÍGUEZ TIRADO, Ana María (Coord). *Cuestiones actuales de Derecho Porcesal*. Tirant Lo Blanch. Valencia. 2017. Pág. 565. Las apreciaciones del autor en este sentido tratan de evitar que *«no se deje abierta la puerta a un filtrado de información periódica de los servidores a las autoridades».*

[438] Vid. RODRÍGUEZ LAINZ, José Luis. «¿Podría un juez español obligar a Apple a …?.» Op. Cit. Págs. 7 y siguientes. El autor analiza una interesante cuestión relacionada con la empresa Apple, muy conocida a nivel mundial por la fabricación de los teléfonos inteligentes conocidos como iPhone. El autor pone de manifiesto la doble condición de la empresa como fabricante de productos, pero también como prestadora de servicios en cuento que ostenta la gestión de aplicaciones como iCloud o iTunes, pero también permite que sus aparatos soporten aplicaciones de mensajería de la que no siendo titular sí que disponen y disfrutan de la encriptación propia de estos dispositivos. El autor concluye en que la legislación española podría ser suficiente a los efectos de poder exigir el acceso al dispositivo, sin embargo, aprecia muy serias trabas a esta posibilidad. Las posibilidades de acceso las descarta como fabricante y manifiesta sus dudas en cuanto a la condición de prestador de servicios.

facilite la practica de la diligencia de registro, bien accediendo al sistema, o dando la asistencia técnica necesaria que permita que los datos se examinen y visualicen.

El párrafo segundo del artículo 588 septies b LECrim, establece nuevas obligaciones a terceros, también concebidas en términos muy abiertos. En este apartado la obligación se dirige a *"cualquier persona"* que pueda conocer el funcionamiento del sistema o de las medidas de protección con las que cuente. Como se puede apreciar, la Ley incluye la imposición de una obligación de hacer, que se concreta en realizar cualquier actividad que sea necesaria para que la diligencia resulte posible, y se impone a cualquiera que, de manera profesional o no, sepa acceder al sistema. Hubiera sido deseable mayor concreción sobre la definición de qué debe considerarse como una persona que conoce el sistema, y si se exige que éste obligado tenga alguna relación legal o profesional con el propietario de dicho sistema, porque llegado el caso podría interpretarse el precepto de una manera tan amplia que permitiera acudirse a los servicios de un "hacker", quien por tener conocimientos técnicos suficientes, pueda acceder a estos sistemas, y conocer su contenido, sólo acreditando dichos conocimientos y amparándose en la exigencia derivada de esta obligación.

Las exclusiones al deber de colaboración impuesto son idénticas en el caso de las dos diligencias. Al igual que en el art. 588 sexies, apartado c, párrafo 5, segundo párrafo LECrim, en esta diligencia de registro de remoto de dispositivos no cabe imponer la obligación de colaboración ni al investigado (lo que resulta derivado del derecho a no confesarse culpable y no declarar contra sí mismo), ni a sus familiares, amparados por el art. 416.1 LECrim, ni tampoco a los afectados por el secreto profesional, debido a las circunstancias por las que conocieron esta información[439].

Junto a la obligación de colaborar (hacer) que se ha descrito, el párrafo tercero del artículo impone, también, el deber de guardar secreto sobre las medidas que hayan sido solicitadas por las autoridades, así como sobre la propia petición de estas.

El artículo no determina el modo en que los agentes solicitantes pueden exigir esta obligación. Sólo se indica que las *"autoridades y agentes encargados de la investigación"* pueden exigir su cumplimiento. Es evidente que para poder exigir un comportamiento, sin que ello sea coactivo, los agentes deberán identificarse ante el obligado, informar, aunque sea sólo de un modo mínimo, acerca de qué es lo que se está buscando, de un modo lo suficientemente concreto, para que el obligado sepa qué datos buscar y analizar, o cómo facilitar el acceso; asimismo, deberá indicarse a

[439] El art. 416. 2 contiene la dispensa en la obligación de declarar del abogado con respecto a los hechos que el investigado le hubiera confiado en calidad de abogado defensor; asimismo, el precepto contiene un nuevo apartado 3 que fue introducido por la Ley Orgánica 5/2015, de 27 de abril, por la que se modifica la Ley de Enjuiciamiento Criminal y la Ley Orgánica 6/1985, de 1 de julio del Poder Judicial. Este apartado dispensa de la obligación de declarar también a los intérpretes y traductores que han podido intervenir en las declaraciones y conversaciones mantenidas entre el abogado y su cliente, referente a los hechos sobre los que han podido tener conocimiento ejercitando esos papeles y funciones de traducción e interpretación.

este obligado que no debe alterar ni destruir el sistema. Estas indefiniciones de la norma pueden ser suplidas en el auto que autorice esta diligencia, de manera que se huya de cualquier arbitrariedad en la ejecución.

El párrafo cuarto del art. 588 septies b) LECrim, dispone con respecto a los "*prestadores de servicios"*, las *"personas señaladas en el art. 588 ter apartado e)"*, los *"titulares y responsables del sistema informáticos o base de datos"*, *así como a cualquier persona que pueda conocer el funcionamiento del sistema o de las medidas pensadas para su protección*, la misma responsabilidad prevista en el art. 588 ter e, apartado 3 LECrim, es decir, la imputación por un delito de desobediencia. Es preferible que el auto que autorice la diligencia y permita recabar ayuda de terceros contenga un apercibimiento expreso sobre este particular.

El art. 588 septies apartado c LECrim prosigue la regulación de la diligencia, pero esta vez en lo que se refiere a las delimitaciones temporales. La naturaleza invasiva de esta diligencia exige que su ejecución no se sostenga indefinidamente en el tiempo, e incluso en el caso en que la investigación lo requiera, tampoco resulta oportuno dilatar indefinidamente su ejecución en el tiempo. El legislador ha limitado la practica de esta diligencia al plazo de un mes, como máximo, sin perjuicio de prórrogas por periodos de un mes, hasta el límite máximo de tres meses. Pasados tres meses como máximo, no cabe ninguna otra prórroga.

En lo relativo a la protección de los derechos de terceros ajenos a las investigaciones, al analizar el contenido art. 588 bis h) LECrim, se vio que quedaba a la regulación de cada una de las diligencias de investigación, el establecimiento de las concretas medidas de protección de estas terceras personas, admitiendo la posibilidad de que los jueces y tribunales acuerden el desarrollo de dichas diligencias, aunque les afecten. El concepto de tercero afectado por la medida abarcaba tanto al titular del equipo como al usuario o usuarios del dispositivo afectado.

El Juez instructor puede acordar en el auto que acuerde la medida de registro remoto todo cuanto guarde relación con estas cuestiones, amparado en la habilitación contenida en el art. 588 septies a, apartado 2 LECrim. Por ello, no resulta extraño que en el ejercicio de esa facultad legalmente reconocida al órgano judicial pueda incluir en el auto el alcance y la forma de acceso al equipo y las medidas que se adoptarán para proteger los datos de terceros ajenos a la investigación.

En lo que se refiere en concreto al contenido de la diligencia de registro remoto de equipos, no hay ninguna regulación especifica que establezca mecanismos de protección dirigidos de manera específica a la protección de los derechos de terceros afectados[440], con lo que todo lo que se refiera

[440] Hay que recordar el contenido de la STS 287/2017, de 19 de abril. Ponente: Don Manuel Marchena Gómez, que ha sido aludida en otras partes de este trabajo y que apunta sobre las posibles implicaciones del uso que se da de un mismo

a esta cuestión se debe regir por los principios generales aplicables a todas las demás diligencias de investigación.

5. Controversias sobre la localización de datos electrónicos ubicados en la nube.

5.1. Concepto de *cloud computing* y regulación legal. Contextualización de la problemática acerca del uso de estos servicios en el ámbito procesal penal.

La tremenda variedad de diligencias de investigación recogidas en la LECrim suscita interesantes interrogantes jurídicos, que vienen derivados de algunos aspectos técnicos que se emplean para su ejecución. En el ámbito procesal penal se exige, más que en otros órdenes jurisdiccionales, una correspondencia estricta entre el contenido previsto en la ley y las concretas facultades derivadas de la aplicación de estas normas. La finalidad que se persigue con ello es evitar aquello que ha venido aconteciendo hasta la promulgación de las leyes procesales que se están analizando, es decir, que la clamorosa ausencia de regulación sobre la investigación criminal mediante el empleo de la tecnología venía suponiendo que se procedía a la realización de cualquier actuación de investigación sin amparo legal, con la finalidad de evitar cualquier efecto no deseado en el proceso[441], sobre todo la nulidad. Por eso, la promulgación de la actual regulación concitó el elogio de los operadores jurídicos, porque al menos, se ponía fin al vacío legal existente.

---

aparato por parte de terceras personas. La sentencia dice que cuando este hecho no es ignorado por parte del autor del ilícito penal admitiendo el uso por parte de terceros, admite que el derecho a su propia intimidad se ve difuminado. El apoyo que usa la resolución para esta idea descansa, según la propia sentencia sostiene en «*el respaldo de una jurisprudencia de esta Sala y del Tribunal Constitucional. En efecto, en nuestra STS 786/2015, 4 de diciembre, con cita de la STC 173/2011, 7 de noviembre, recordábamos que « ...el consentimiento eficaz del sujeto particular permitirá la inmisión en su derecho a la intimidad, pues corresponde a cada persona acotar el ámbito de intimidad personal y familiar que reserva al conocimiento ajeno (SSTC 83/2002, de 22 de abril, FJ 5 ; 196/2006, de 3 de julio , FJ 5), aunque este consentimiento puede ser revocado en cualquier momento (STC 159/2009, de 29 de junio , FJ 3). Ahora bien, se vulnerará el derecho a la intimidad personal cuando la penetración en el ámbito propio y reservado del sujeto «aún autorizada, subvierta los términos y el alcance para el que se otorgó el consentimiento, quebrando la conexión entre la información personal que se recaba y el objetivo tolerado para el que fue recogida» (SSTC 196/2004, de 15 de noviembre, FJ 2 ; 206/2007, de 24 de septiembre, FJ 5 ; 70/2009, de 23 de marzo , FJ 2). En lo relativo a la forma de prestación del consentimiento, hemos manifestado que este no precisa ser expreso, admitiéndose también un consentimiento tácito. Así, en la STC 196/2004, de 15 de noviembre , en que se analizaba si un reconocimiento médico realizado a un trabajador había afectado a su intimidad personal, reconocimos no sólo la eficacia del consentimiento prestado verbalmente, sino además la del derivado de la realización de actos concluyentes que expresen dicha voluntad (FJ 9). También llegamos a esta conclusión en las SSTC 22/1984, de 17 de febrero y 209/2007, de 24 de septiembre , en supuestos referentes al derecho a la inviolabilidad del domicilio del art. 18.2 CE , manifestando en la primera que este consentimiento no necesita ser «expreso» (FJ 3) y en la segunda que, salvo casos excepcionales, la mera falta de oposición a la intromisión domiciliar no podrá entenderse como un consentimiento tácito (FJ 5)*».

[441] Se ha mencionado en varias ocasiones a lo largo de este trabajo la figura del Anteproyecto de Código Procesal Penal como intento de sustituir la actual regulación por otra distinta. En dicha norma se avanzaba en el modelo de instrucción, que se daba al Ministerio Fiscal, sustituyendo al Juez de instrucción en su misión tuitiva de los derechos fundamentales,

En todo caso, cualquier actividad legislativa no está exenta de imperfecciones técnicas, algunas de las cuales se ponen de manifiesto una vez promulgada la ley. En el caso de la nueva regulación sobre diligencias de investigación electrónica, aunque puede decirse que es abrumadoramente exhaustiva y variada, en materia de acceso y registro a datos alojados en sistemas de almacenamiento virtual resulta difusa. Por eso, en esta parte del trabajo se analiza si la regulación sobre el registro de los datos alojados en la "*nube*" [442] está debidamente regulada en la ley, y si su contenido es suficiente, así como también, si se originan problemas en su aplicación, que es una cuestión de una evidente dimensión práctica.

El hecho de que para realizar una actividad delictiva se pueda acudir al empleo de la nube como medio para guardar datos es una muestra de la capacidad de toda actividad delictiva para adaptarse y valerse de su entorno. El empleo de la tecnología aplicada a la criminalidad, es una realidad que ha tenido a remolque la actividad legislativa de los Estados, que han debido adaptarse a ella, creando tipos penales que no pueden sustraerse de que, en la redacción de su tipo objetivo, se aluda al empleo de sistemas, medios y mecanismos tecnológicos.

La tecnología permite la remisión de datos de todas las clases y formas y, por supuesto, cabe que alguno de estos datos permita acreditar la comisión, la participación o cualquier otro indicio relacionado con algún tipo penal concreto[443], y por eso resulta necesario poder acceder a dichos datos, cualquiera que sea el lugar en que estén alojados[444].

En suma, el empleo de la tecnología en el ámbito de la delincuencia es cada vez más intenso y frecuente, y, además, de forma complementaria, también permite compartir y difuminar la información generada por tales actos ilegales, con la finalidad de ocultar el delito, o de dificultar la averiguación del hecho y la determinación del responsable. Teniendo presente que toda la

---

por una nueva figura, el Juez de Garantías. Puede consultarse su texto en el enlace del Ministerio de Justicia: http://www.mjusticia.gob.es/cs/Satellite/Portal/1292375190463?blobheader=application%2Fpdf&blobheadername1=Content-Disposition&blobheadername2=Medios&blobheadervalue1=attachment%3B+filename%3DCODIGO_PROCESAL_PENAL.pdf&blobheadervalue2=1288778173060

[442] A efectos de dejar constancia de la importancia que cobra desde un punto de vista social la creciente importancia del alojamiento de datos fuera de un servidor propio y cómo ello se sustituye por el *cloud computing* o nube haremos alusión al siguiente artículo de actualidad publicado muy reciente en EL PAIS. Arenas. Guillermo. "¿Donde se guarda lo que subes a la nube?". EL PAIS. Sección Tendencias. Perteneciente a la revista RETINA. Edición digital 11 de enero de 2018. https://retina.elpais.com/retina/2018/01/11/tendencias/1515662157_635397.html

[443] Pondremos como ejemplo por reciente la STS 167/2016, de 2 de marzo. Ponente: Don Juan Saavedra Ruíz, en la que se condena por un delito de posesión con facilitación de material pornográfico del art. 189.1.b) del CP, en el que resulta trascendental el empleo de un ordenador y el intercambio de archivos en las redes.

[444] A modo de ejemplo, una conversación de naturaleza sexual con un menor puede quedar recogida en un archivo de audio o de video, o unas amenazas graves pueden realizarse por escrito usando Facebook; fotografías vejatorias que pudieron hacerse empleando un móvil, y subiendo su contenido a la red, o una conversación intimidatoria, efectuada mediante un chat de video, como por ejemplo Skype, o la acción de compartir fotografías de menores, en clara actitud sexual, mediante programas *peer to peer*, son acciones penadas por la ley, y que para ser acreditadas necesitan que se aporten a las actuaciones los datos en que las mismas quedan reflejadas.

información es fácilmente transmisible, esta cualidad de la misma hace que se convierta en un objeto volátil y de fácil manejo, que permite que un acto ilícito pueda realizarse desde nuestro país hacia fuera de nuestras fronteras y viceversa.

La facilidad de transmisión de los datos electrónicos, de modo casi inmediato, se debe a la existencia de dispositivos muy sofisticados, y de *software* cada vez más sencillo de ejecutar mediante las ya familiares *apps*. Entre la nueva gama de servicios nacidos a la luz de la tecnología, cabe detenerse ahora, en aquellos que ofrecen el alojamiento de datos en servidores situados en puntos geográficos muy distintos y distantes. Es evidente que una investigación criminal puede necesitar de estos datos, por ser sensibles o relevantes en los hechos investigados.

Los datos electrónicos pueden ser considerados, en algunas ocasiones, el bien objeto del delito, el bien jurídico protegido, el beneficio obtenido mediante ataques informáticos, etc. Estos datos pueden guardarse en la nube, y ser atacados en ella, lo que constituye incluso un ilícito penal[445] actualmente previsto en la ley [446].

Otro aspecto a tener en cuenta en esta materia es la concurrencia de las personas jurídicas en el uso de medios tecnológicos, y también en la comisión delictiva. Las ventajas que las personas jurídicas presentan en el orden civil, basada en la creación de patrimonios separados de sus dueños reales, se superponen a su capacidad de rápida actuación en el tráfico, y a ventajas fiscales, además son creadoras, transformadoras, y comercializadoras de datos. En la actualidad, la ley penal las convierte en sujetos activos y pasivos de delitos, y por ello el legislador, les impone la obligación de realizar un esfuerzo considerable para evitar el empleo de sus medios materiales en la realización de actos penales, y que se cometan por sus empleados, a veces usuarios de dispositivos tecnológicos propiedad de la persona jurídica que las emplea[447].

---

[445] CATÀ FIGULS, Josep. Entrevista a Gil Shwed: «Los ciberataques se fijarán en la nube, no en los dispositivos». *Revista Electronica Retina, Diario El País*. Barcelona 5 febrero 2018 - 09:51 CET. Puede consultarse el texto integro en el siguiente enlace: https://retina.elpais.com/retina/2018/02/02/innovacion/1517585688_626052.html

[446] La Ley orgánica 1/2015, de 30 de marzo que modificó el Código Penal, introdujo las figuras de los delitos informáticos bajo la rúbrica dedicada a los delitos contra la revelación de secretos. En concreto el art. 197 bis 1 castiga con prisión de seis meses a dos años el acceso al conjunto o a una parte de un sistema de información.

[447] No ha de olvidarse el contenido del actual artículo 31. bis 4 y 5 del Código Penal en la versión dada por la Ley Orgánica 1/2015 de 30 de marzo. A tenor de ella las personas jurídicas «*4. Si el delito fuera cometido por las personas indicadas en la letra b) del apartado 1, la persona jurídica quedará exenta de responsabilidad si, antes de la comisión del delito, ha adoptado y ejecutado eficazmente un modelo de organización y gestión que resulte adecuado para prevenir delitos de la naturaleza del que fue cometido o para reducir de forma significativa el riesgo de su comisión. En este caso resultará igualmente aplicable la atenuación prevista en el párrafo segundo del apartado 2 de este artículo.5. Los modelos de organización y gestión a que se refieren la condición 1.ª del apartado 2 y el apartado anterior deberán cumplir los siguientes requisitos:1.º Identificarán las actividades en cuyo ámbito puedan ser cometidos los delitos que deben ser prevenidos.2.º Establecerán los protocolos o procedimientos que concreten el proceso de formación de la voluntad de la persona jurídica, de adopción de decisiones y de ejecución de las mismas con relación a aquéllos.3.º Dispondrán de modelos de gestión de los recursos financieros adecuados para impedir la comisión de los delitos que deben ser prevenidos.4.º Impondrán la obligación de informar de posibles riesgos e incumplimientos al organismo encargado de vigilar el funcionamiento y observancia del modelo de prevención.5.º*

La exposición de esta multiplicidad de visiones que implica el uso de los datos informáticos hace que la siguiente fase del estudio se dirija al concepto de *cloud computing*, a la regulación que sobre ella exista, y a la visión procesal penal de la misma. Esto se hará mediante su relación con las diligencias de acceso y registro de datos.

5.1.1. Concepto de *cloud computing*.

La denominada nube, o el *cloud computing,* se define por la doctrina que la ha estudiado como *«un modelo que permite el acceso desde cualquier lugar y bajo demanda a una serie de recursos informáticos compartidos y configurables (redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente aprovisionados y puestos en funcionamiento con un mínimo esfuerzo de gestión e interacción con el proveedor de servicios»* [448].

Las distintas definiciones, que se vienen utilizando en los diversos estudios jurídicos existentes sobre esta materia, no son, en general, muy diferentes, pues la describen como aquel «*modelo que permite, de forma práctica y desde cualquier ubicación, el acceso bajo demanda a una serie de recursos informáticos configurabas compartidos (redes, servidores, sistemas de almacenamiento, aplicaciones y servicios), que pueden ser rápidamente dotados y puestos en funcionamiento con un mínimo esfuerzo de gestión e interacción con el proveedor de servicios»*[449]. Sin embargo, también se pueden encontrar en la doctrina otras definiciones de este servicio que pueden ayudar a una mejor comprensión del concepto[450].

En el plano normativo, la Directiva 2016/1148 de 6 de julio de 2016 *«entiende por «servicios de computación en nube» aquellos servicios que permiten acceder a un conjunto modulable y elástico de recursos informáticos que se pueden compartir. Esos «servicios de computación» incluyen*

Establecerán un sistema disciplinario que sancione adecuadamente el incumplimiento de las medidas que establezca el modelo.6.º Realizarán una verificación periódica del modelo y de su eventual modificación cuando se pongan de manifiesto infracciones relevantes de sus disposiciones, o cuando se produzcan cambios en la organización, en la estructura de control o en la actividad desarrollada que los hagan necesarios». Por lo tanto, el llamado "compliance penal", o auditoría de procesos en los que pueden advertirse la comisión de ilícitos en una persona jurídica no podrá olvidar el empleo de los ordenadores, servidores, y dispositivos de la empresa como elementos que pueden servir para la comisión de un delito.

[448] Cfr. CUESTA, José Luis. «Cloud, una oportunidad para la Administración Pública». *Estrategia Financiera*, Nº 292, 28 de Febrero de 2012. LA LEY 2017/2012. Pág. 1. El autor a su vez toma la definición que es ofrecida por el Instituto Nacional de Estándares y Tecnología de Estados Unidos.

[449] Cfr. GARCÍA SÁNCHEZ, Manuel. «Retos de la computación en la nube» en MARTÍNEZ MARTÍNEZ RICARD (Editor), *Derecho y Cloud Computing.* Thomson Reuters- Aranzadi. Pamplona. 2012. Pág. 40. El autor en su obra cita una traducción del inglés de la definición del servicio de computación en la nube extraída del Instituto de Estándares y tecnologías, comúnmente denominado NIST.

[450] Vid. MARTÍNEZ MARTÍNEZ, RICARD. «El derecho y el Cloud computing» en MARTÍNEZ MARTÍNEZ RICARD (Editor), *Derecho y Cloud Computing.* Thomson Reuters- Aranzadi. Pamplona. 2012. Pág. 17.

recursos tales como las redes, servidores u otras infraestructuras, sistemas de almacenamiento, aplicaciones y servicios. El término «modulable» se refiere a los recursos de computación que el proveedor de servicios en nube puede asignar de manera flexible con independencia de la localización geográfica de los recursos para hacer frente a fluctuaciones de la demanda. El término «elástico» se usa para describir los recursos de los que se abastece y que se ponen a la venta según la demanda, de modo que se puedan aumentar o reducir con rapidez los recursos disponibles en función de la carga de trabajo. La expresión «que se pueden compartir» se usa para describir recursos informáticos que se proporcionan a múltiples usuarios que comparten un acceso común al servicio pero la tramitación se lleva a cabo por separado para cada usuario, aunque el servicio se preste desde el mismo equipo electrónico»[451].

La primera nota que resulta común a todas las definiciones anteriores es que se trata de un servicio ofertado por empresas especializadas, que consiste en el alojamiento de información a la que se accede mediante el uso de diferentes aplicaciones y sistemas. Para acceder a ella no se requiere más que una conexión a internet, destacando como una de sus mejores ventajas, el poder llegar hasta ella de manera remota, desde cualquier lugar, siendo característico de esta clase de servicios, el que esta información no está en el lugar desde el que se visualiza, o se emplea para trabajar con ella o intercambiarla, en suma, no está en la memoria del ordenador.

La segunda característica de la nube es que no necesita emplear un material adicional para guardar y recuperar la información desde servidores que necesitan un mantenimiento costoso, a unas instalaciones que los guarden. La información está alojada en los servidores propiedad de las empresas que ofrecen el servicio y el ordenador del usuario funciona como una ventana de acceso a la información. Para acceder se suele usar una cuenta con un nombre de usuario y una contraseña de acceso.

En tercer lugar, es un servicio que permite que varios usuarios intercambien y modifiquen los datos alojados en dichos servidores.

Es un servicio muy cómodo que permite emplear múltiples dispositivos, por distintas personas, y tener la plena disposición, en cualquier momento, y en cualquier lugar con acceso a la red, toda la información necesaria, trabajar sobre ella, compartirla, etc. Además, no ocupa espacio, porque la información no está dentro del dispositivo empleado, sino que es solo una puerta de acceso a los servicios descritos[452]en servidores situados en otro lugar.

[451] Considerando número 17. La Directiva regula las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.
[452] Las notas que le son atribuidas desde un punto de vista técnico son *«el autoservicio bajo demanda, el acceso a través de la red, la agrupación de recursos, la flexibilidad y el servicio sujeto a medida»* (Cfr. GARCÍA SÁNCHEZ. «Retos

Los técnicos informáticos distinguen entre diferentes clases de nube, siguiendo criterios como el tipo de usuario, su agrupación en comunidades más o menos abiertas, etc. Pero en todo caso la característica esencial de la nube es la misma: la ausencia de ubicación tanto de la información como de las herramientas de trabajo utilizadas en el lugar en que esto se lleva a cabo[453]

El uso de los servicios en la nube crece cada día más en todos los ámbitos, desde el que le dan los poderes públicos para diversos usos y finalidades[454] y para facilitar a los el cumplimiento de sus obligaciones[455], hasta el que se realiza en el ámbito privado, en el que el empleo de los datos configuran una oportunidad de negocio[456]. Es probablemente dentro del uso privado de los datos donde presenta mayor interés la investigación de la actividad delictiva que pueda desarrollarse en la nube, lo que conlleva que el Estado haya desarrollado los medios legislativos necesarios para la investigación de los delitos dentro de ese ámbito virtual.

Lo que está fuera de toda duda es que en un sector de la investigación criminal dirigida al registro y análisis de datos virtuales, si la protección que brindan los Estados fuera lo más internacionalizada y armonizada posible, se obtendría una mejor protección de los datos que están transmitiéndose de un punto a otro de las redes de información e igualmente se conseguiría una mejor investigación de las

---

de la computación en la nube» en MARTÍNEZ MARTÍNEZ RICARD (Editor), *Derecho y Cloud Computing.* Op. Cit. Pág. 41).

[453] Se habla de nubes privadas, nubes públicas, nubes en comunidad, y nubes híbridas, que se diferencian por el uso enteramente exclusivo del usuario (las privadas) hasta el empleo abierto de lo depositado en ella (las públicas), pasando por el uso de la misma nube por parte de distintas organizaciones (en comunidad), o la utilización por diversos usuarios de modo individualizado. La distinción es realizada por GARCÍA SÁNCHEZ, Manuel. «Retos de la computación en la nube» en MARTÍNEZ MARTÍNEZ RICARD (Editor), *Derecho y Cloud Computing.* Op. Cit. Pág. 43.

[454] A mero título ejemplificativo de la importancia que presenta la materia en el ámbito de la Unión Europea puede consultarse en la página web de la Comisión, bajo el criterio de búsqueda cloud computing, la ingente cantidad de empresas que cuentan entre su objeto social con esta clase de actividades y que se han ido inscribiendo dentro del Registro de los denominados "Grupos de Interés", que no son otra cosa que la formalización como Lobby de las empresas de estas características a los efectos de poder influir en el contenido de las distintas normas que se promulguen dentro de la UE sobre este particular, lo que da sobradamente cuenta de la importancia que esta materia representa para distintas entidades: http://ec.europa.eu/geninfo/query/index.do?QueryText=cloud+computing&op=Búsqueda&swlang=es&form_build_id=form-8TH_3SB4zIhUh8wzOYfTXbsBey2Lhd-3Fpqc-pz4-60&form_id=nexteuropa_europa_search_search_form.

[455] Pensemos en acceso de un ciudadano a los servicios públicos de empleo para solicitar una prestación o subsidio, la posibilidad de abonar una multa de tráfico de través de internet, inscribirnos en una convocatoria pública a una oposición, pedir una cita médica, pagar los impuestos y presentar las declaraciones tributarias etc., Son todos estos actos cotidianos una cuestión que se hace cada vez más corriente en nuestro día a día. Todas ellas son posibles y vienen auspiciadas por Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, que regula en la actualidad las relaciones de los ciudadanos con la Administración, derogando así el contenido de la Ley 11/ 2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

[456] A modo de ejemplo y con la finalidad de que el lector comprenda el interés económico del mercado de datos se cita un breve extracto del Informe de la Comisión Europea en el que realiza una propuesta de reglamento relativo a un marco para la libre circulación de los datos no personales en la Unión Europea, de fecha 13 de septiembre de 2017. Dicho informe dice textualmente: «*Tal como se indica en la Comunicación de 2017 «La construcción de una economía de los datos europea»2, el valor del mercado de los datos de la UE se estimó en 2016 en casi 60. 000 millones EUR, lo que representa un incremento del 9,5 % con respecto a 2015. Según un estudio, el mercado de los datos de la UE podría posiblemente ascender a más de 106.000 millones EUR en 2020*».

actividades delictivas que se puedan producir aprovechando este trasiego de información entre distintos puntos geográficos[457].

5.1.2. Normativa reguladora del *Cloud computing*.

Una vez que se ha expuesto el concepto de *cloud computing*, y que ha sido vista la trascendencia que esta actividad tiene en la actualidad, así como también su importancia económica, cabe analizar si existe alguna normativa que la regule.

Sobre esta materia se puede afirmar desde este instante que no hay regulación especializada, y las menciones que se dan sobre esta figura en algunas normas resultan testimoniales, dejando de lado el Considerando 17 de la Directiva 2016/1148 de 6 de julio de 2016, ya mencionado en el apartado anterior.

La ausencia de regulación especializada tiene sentido en la medida en que se trata de una actividad mercantil, desarrollada por parte de empresas especializadas, normalmente en el ámbito de las telecomunicaciones o servicios en internet. En todo caso, estas empresas no dejan de ser entidades mercantiles, que se constituyen, desarrollan y funcionan dentro del marco establecido por las distintas legislaciones nacionales sobre constitución y funcionamiento de empresas mercantiles en general[458]. Por eso, desde un punto de vista mercantil no se justifica una legislación que imponga algún condicionante específico o propio para esta clase de empresas, como pudiera existir para otro tipo de entidades como los bancos, las compañías de seguros o las empresas que se dedican a prestar los servicios de trabajo temporal, que están condicionadas legalmente a exigencias de determinados niveles de capital. Las empresas que presten, entre sus servicios, los propios del *cloud computing,* no se deben diferenciar por la forma societaria o por los niveles de capital de las demás. Su diferencia está en el objeto material de su actividad, que es el uso y tratamiento de la información que almacenan. Por lo tanto, son entidades que deben respetar la legislación sobre protección de datos y sus exigencias sobre el uso mercantil de los datos como objeto de comercio.

[457] *Diario Cinco Días*. «Bruselas acaba con las fronteras nacionales de la nube digital». Bruselas / Madrid 18 SEP 2017 - 07:42 CEST. Se puede consultar la integridad de la noticia en el siguiente enlace:https://cincodias.elpais.com/cincodias/2017/09/15/companias/1505497536_740023.html?por=mosaico

[458] En la legislación española, la norma que regula la creación y el funcionamiento de las distintas empresas mercantiles, es el Real Decreto Legislativo 1/2010, de 2 de julio, por el que se aprueba el texto refundido de la Ley de Sociedades de Capital.

La protección de datos, en cambio, si que cuenta con un marco regulatorio rico y muy variado, compuesto tanto por normas europeas, recientemente modificadas [459], y también por leyes nacionales, adaptadas a las normas europeas referidas[460]. Ambos grupos de disposiciones tienen por finalidad la protección de los datos personales, lo que se configura y reconoce como un derecho fundamental.

Los datos no reciben siempre el mismo grado de tutela, pues hay datos que tienen un nivel especial protección, como el caso de los datos personales del individuo, y otros que simplemente cumplen una función comercial o mercantil, y que no están protegidos. Este segundo tipo de datos, al ser considerados como un simple objeto de comercio, no reciben un tratamiento legal especial ni cuentan con una regulación especial sobre la actividad que tiene que ver con su uso y tratamiento y por consiguiente no alcanzan al grado de protección de los primeros.

En los siguientes apartados se analizará el contenido de varias normas, tanto europeas como nacionales, sobre la protección de datos; aunque esto se hará con la finalidad de buscar en ellas menciones a la actividad de alojamiento de datos en la nube, de manera que pueda extraerse información que ayude en la mejor configuración de estos dispositivos como objeto de registro.

5.1.2.1. La normativa europea sobre protección de datos. La figura del Fiscal Europeo y su relación con el uso de datos, el empleo de la nube y las diligencias de investigación electrónicas.

Las instituciones europeas han mostrado una gran iniciativa en la redacción de normas sobre la protección de datos personales. La efectiva protección de los datos personales de los ciudadanos se configura como un derecho expresamente reconocido dentro del acervo de normas creadoras de las instituciones europeas, y por eso están obligadas a desarrollar un cuerpo legal común para todos los países de la Unión que proteja éste y otros derechos relacionados. El objeto de protección en todos los casos, son los datos estrictamente personales, en la medida que la regulación permite concentrarlos mediante servicios de alojamiento, y tratamiento de datos en general. Por

[459] A nivel europeo debe reseñarse el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general).

[460] A nivel interno, las normas que cabe destacar son la Ley Orgánica 3/2018, de 5 de diciembre, reguladora de la Protección de datos personales y garantías de derechos digitales, que deroga la Ley Orgánica de Protección de datos de carácter personal 15/1999, de 13 de diciembre; la Ley 34/2002 de servicios de la sociedad de la información y de comercio electrónico y el RDL 5/2018, de 27 de julio de medidas urgentes de adaptación del derecho español a la normativa europea en materia de protección de datos.

consiguiente, es el tipo de dato ante el que estemos el que marca la regulación y la protección aplicables a cada uno de ellos[461].

En este apartado se trata de analizar qué normas de la Unión Europea rigen en el ámbito de la protección de datos y qué relación puede haber entre el contenido de las mismas y las operaciones propias de las actividades propias del *cloud computing.* Es precisamente la enorme facilidad que tienen los datos para ser transmitidos de un lugar a otro, una de las razones que justifica que sea la regulación europea la que impulsa su tutela y protección por encima de cualquier otra legislación nacional[462].

La regulación europea cuenta con varias normas protectoras de los datos personales, siendo el Reglamento europeo 2016/679, de 27 de abril de 2016, que entró en vigor el 25 de mayo de 2018[463] y que deroga la Directiva 95/46, la norma de carácter general y supletoria de todas las demás, que dota de contenido los derechos del art. 8.1 de la Carta de los Derechos Fundamentales de la Unión Europea, y del art. 16.1 del Tratado de Funcionamiento de la Unión Europea, que recogen como derecho esencial de los ciudadanos europeos el de la protección de datos de carácter personal. Además el contenido de este derecho debe enlazarse con una mejora en los sistemas de protección de los mismos, resultando esencial, en este sentido, el Tratado de Ámsterdam, que es el instrumento legal creador del Espacio de Libertad, Seguridad y Justicia de la Unión Europea[464], y que sirve para

[461] Las normas reguladoras de datos en el ámbito de la Unión Europea son las siguientes: Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DO L 119 de 4.5.2016, p. 1); la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (DO L 119 de 4.5.2016, p. 89); y en tercer lugar Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) (DO L 201 de 31.7.2002, p. 37).

[462] Como se ha dicho la normativa en la actualidad está conformada por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DO L 119 de 4.5.2016, p. 1). En contraposición a la regulación sobre los datos que no tienen la condición de carácter personal existe una propuesta de reglamento del Parlamento Europeo y del Consejo relativo a un marco para la libre circulación de datos no personales en la Unión Europea. Dicha propuesta fomenta «*el principio de libre circulación de datos no personales en la Unión"* y según se indica "*El marco jurídico relativo a la protección de las personas físicas en lo que atañe al tratamiento de datos personales, en particular el Reglamento (UE) 2016/679, la Directiva (UE) 2016/680 y la Directiva 2002/58/CE, no debe verse afectado por el presente Reglamento*» (pág. 13 de la propuesta).

[463] Art. 51 del Reglamento.

[464] Sobre dicho particular destacan los principios de confianza mutua, armonización de ordenamientos, reconocimiento recíproco de resoluciones judiciales y reforzamiento de la cooperación policial y judicial trasnacional. En relación con todos estos principios véase Vid. HOYOS SANCHO, Montserrat. «Armonización de los procesos penales, reconocimiento mutuo y garantías esenciales», en HOYOS SANCHO, Montserrat (Coord). *El proceso penal en la Unión Europea: garantías esenciales.* Instituto de Estudios Europeos, Lex Nova. Valladolid. 2008. Pág. 42.

que el territorio europeo se dote de unos sistemas que hagan efectiva la protección de los derechos y que se unifiquen los mismos dentro del territorio.

Junto al Reglamento 2016/679, de 27 de abril de 2016, hay otra norma que se encarga de regular la protección de los datos personales de las personas físicas, aunque de manera específica en lo que se refiere a la investigación penal. Se trata de la Directiva 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en los que respecta al tratamiento de los datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/1977/JAI del Consejo.

La simple existencia de estas normas permite concluir que para las instituciones europeas la protección de datos se erige como un aspecto irrenunciable dentro del marco de derechos que conforman el catálogo de derechos fundamentales de la Unión Europea. El análisis de estas normas permitirá delimitar el grado de protección que deben tener los datos que se depositan o alojan mediante el empleo de los servicios de *cloud computing*, y de modo más concreto aquéllos datos que puedan ser de interés para la investigación penal.

El análisis del contenido del Reglamento 2016/679, de 27 de abril de 2016, permite constatar que en dicha norma no hay ninguna regulación específica de los servicios en la nube, aunque sí que se regulan las actividades de tratamiento de datos, entre las que se incluyen la transferencia de datos personales de personas físicas por parte de los operadores. En el Reglamento el tratamiento de la información se configura como el acto que consiste «*en cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción*»[465].

Por consiguiente, aunque no hay una regulación específica de los servicios en la nube y de actividades similares, lo que ha sido calificado como decepcionante por la doctrina[466], sí que hay

[465] Art. 4, apartado 2 del Reglamento.

[466] Cfr. SOLAR CALVO, Puerto. Op. Cit. Pág. 13 y 14. El autor alude que el imparable avance tecnológico deja atrás al legislador comunitario y que aspectos tales como el Internet de las cosas o el BITech no se han regulado, razón por la que augura que será necesaria una nueva normativa. Destaca expresamente *«que el sector destaca que el Reglamento no contempla específicamente cuestiones como el Big Data, el Cloud Computing, el Internet de las cosas o BiTech. Parece que se ha perdido una ocasión para adaptar completamente la norma al entorno digital para permitirla envejecer bien. Finalmente, se critica el hecho de que el pequeño empresario, que es el mayoritario dentro y fuera de nuestro país, es el gran olvidado de esta norma, para cuyo cumplimiento, a pesar de la eliminación de ciertas trabas*

una normativización de algunos de los aspectos fundamentales de esta figura, en especial, la transferencia de los datos entre distintos puntos, lo que constituye la esencia misma del *cloud computing*. Esta transferencia de datos constituye el elemento fundamental de esta actividad en tanto que, resumidamente, ésta consiste en una operación en la que el usuario deposita los datos que son elegidos por él dentro de los servidores ofertados por la empresa suministradora, y propiedad de la misma, en virtud de la ejecución de un contrato de prestación de estos servicios y el documento de autorización que suscribió. La empresa transfiere los datos a unas instalaciones en las que los aloja y desde los que el usuario los consulta. Pero, además, por razones operativas, el suministrador puede transferirlos de dichas instalaciones a otras o incluso subcontratar el servicio de alojamiento con terceros.

En todo caso, el Reglamento no abarca dentro del ámbito de protección a todos los datos, sino que sólo protege, de entre los datos transferidos, el dato que es considerado como personal. Hay datos cuyo tratamiento está completamente prohibido: como los de naturaleza muy sensible, por ejemplo, los genéticos, biométricos (que permiten identificar a una persona de forma indubitada), los referentes a la salud, la vida y la orientación sexual, el origen étnico, y similares[467]. Estos datos, se encuentran especialmente protegidos, y por eso sólo se pueden transferir ante situaciones muy determinadas, y ante situaciones de urgencia como los derivados de la necesidad de proteger intereses vitales o cuando estos datos ya se han hecho públicos[468].

En lo que más interesa al ámbito penal sobre el que se desarrolla este trabajo, el Reglamento también excluye de su ámbito de protección las actividades de empleo y tratamiento de datos personales que las personas físicas realicen de manera personal o doméstica, considerando como tales «*la correspondencia y la llevanza de un repertorio de direcciones, o la actividad en las redes sociales y la actividad en línea realizada en el contexto de las citadas actividades»*[469]. Esta exclusión es muy importante si se analiza y se enfoca a la actividad delictiva, que es el marco que encuadra este trabajo, porque muchos de los datos que son de interés para la investigación criminal, en la mayoría de las ocasiones, pueden situarse precisamente dentro de este ámbito.

En consecuencia, puede afirmarse que el Reglamento carece de una regulación general de las actividades de *cloud computing*, y que las materias que regula que pudieran presentar alguna relación con este tipo de actividad, como lo son específicamente las transferencias de datos a

---

burocráticas y la adaptación al riesgo específico que su actividad presente, estará obligado a solicitar continuo asesoramiento».

[467] Art. 9.1 del Reglamento.

[468] Todas las situaciones vienen descritas en los apartados a) hasta j) del párrafo 2 del art. 9 del Reglamento.

[469] Considerando 18 del Reglamento, puesto en relación con el contenido del art. 2. 2, apartado c) del Reglamento.

terceros lugares, quedan expresamente excluidas de su ámbito de aplicación cuando dichas transferencias se refieran a las actividades personales de un individuo.

En suma, puede decirse que existe una laguna legal en lo que se refiere al ámbito de las trasferencias de datos personales realizadas por los propios individuos en su ámbito particular, sector en el que suele circunscribirse la actividad delictiva, y en el que más pudiere resultar de interés para la instrucción penal el registro de las nubes virtuales en las que se deposita información. Esta ausencia de regulación, y más específicamente para esa concreta acción personal, favorece y facilita que los datos de interés para la instrucción puedan quedar al margen de los controles que se instituyen en las normas europeas para garantizar la protección de los datos personales. Esta ausencia de control constituye una dificultad añadida a la hora de localizar la ubicación de este tipo de datos.

Esta aparente claridad en lo referente a la clasificación de datos, y a su función, colisiona con los *«abundantes conceptos jurídicos indeterminados»*[470] que a veces se emplean en el Reglamento, lo que genera dudas de aplicación en algunos casos. Por ejemplo, si una persona física realiza el depósito de determinados datos personales en la nube, se puede plantear si es o no una actividad en línea, y por lo tanto entrar en el ámbito de protección.

El único contenido del Reglamento que guarda relación directa con una parte de la actividad del almacenamiento en la nube es la exhaustiva y pormenorizada regulación acerca de los flujos trasnacionales de datos[471]. Estas transferencias de datos se regulan en el Capítulo V[472], bajo el principio general de libertad de transferencia de los datos que hayan sido objeto de tratamiento, o bien vayan a serlo. Esta libertad se condiciona a que se verifique el cumplimiento de los niveles de protección exigidos y las condiciones de transferencias a terceros estados previstos legalmente.

El Reglamento diferencia entre los países que están dentro de la Unión, a los que les supone que cumplen con los estándares de protección adecuados, de los que no pertenecen a ésta. En el segundo caso, el proceso de transferencia se somete a autorización por parte de la Comisión, que verificará las condiciones de seguridad en el tratamiento de los datos personales en los lugares, países u organizaciones internacionales a los que vayan a ser transferidos los datos. Se protegen así, tanto la primera transferencia, como las ulteriores entre países u entes terceros[473], y se atenderá siempre al

[470] Cfr. SOLAR CALVO, Puerto. «La protección de datos en la UE: recapitulación de novedades». *Revista Aranzadi Unión Europea* num.1/2017. Pág. 13. BIB 2017\10603. Pág. 13.
[471] Considerando 101 a 117 del Reglamento.
[472] Dentro de dicho capítulo se encuentran los artículos 44 a 50.
[473] Así se desprende del contenido de los considerandos 101 a 104, 107, 108 y 110 a 112, 114 y 116 del Reglamento, puesto en ello en relación con el contenido del Capítulo V.

grado de protección que se otorga a los datos en los lugares a los que son transferidos, para dar dicha autorización o para mantenerla.

En lo que se refiere a la diligencia de investigación que analizamos, estas medidas sólo pueden resultar de utilidad en la medida en que los datos que se estén intentando analizar sean susceptibles de tratamiento al amparo de este Reglamento, lo que, de ser así, y al serle de aplicación el contenido de esta norma coadyuvaría a facilitar su localización, dado que al tener que cumplir con los requisitos que el Reglamento exige, será más sencilla su trazabilidad y localización. Además, a esa mayor facilidad de localización contribuye el que la norma haga depender la transferencia de datos de un contrato privado, por el que el usuario permite la transferencia de estos datos dentro de la Unión o fuera de ella, pero siempre sometido a los condicionantes de protección que recibirá en el lugar de destino.

La segunda norma con relevancia en la protección de datos de carácter personal y también con los alojados en la nube, y que tiene relevancia en la investigación criminal, es la *Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales.* El contenido de esta Directiva debía trasponerse a los ordenamientos nacionales a los dos años de su aprobación[474], hecho éste que no se ha producido en España hasta la fecha y que debió suceder en todo caso antes del 6 de mayo de 2018[475]. Ello implica que existe ciertas dudas acerca del modo en que deben ejercerse por las personas afectadas, los derechos expresamente reconocidos por la Directiva. En todo caso mientras se produce la trasposición existen medidas temporales para paliar esta ausencia[476].

El ámbito de aplicación de esta Directiva se dirige a la protección de los datos de las personas físicas[477], obtenidos durante una investigación penal [478], así como de los obtenidos por la ejecución

[474] Considerando 96 de la Directiva.
[475] Así expresamente se indica en el Acuerdo de Pleno del Consejo General de Poder Judicial de 25 de abril de 2018 que aprobó un informe sobre la Ley Orgánica sobre utilización de datos del registro de nombres de pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves. Pág. 88.
[476] Sobre esta concreta norma, la Ley Orgánica 3/2018, de 5 de diciembre, dispone en su Disposición Transitoria Cuarta que: «*Los tratamientos sometidos a la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, continuarán rigiéndose por la Ley Orgánica 15/1999, de 13 de diciembre, y en particular el artículo 22, y sus disposiciones de desarrollo, en tanto no entre en vigor la norma que trasponga al Derecho español lo dispuesto en la citada directiva*».
[477] Los datos que se obtengan deben siempre ser exactos, completos y actualizados, de manera que conforme al Considerando 32 de la Directiva, cuando no lo sean, no podrán ser objeto de transmisión a cualquiera de los países a los que pudiera resultar de utilidad.

de resoluciones de la misma naturaleza, incluyendo cualquier clase de actividad realizada por parte de cualquier clase de entidad pública dirigida a la investigación, prevención, detección, enjuiciamiento de delitos, así como las actividades también dirigidas a mantener la seguridad colectiva[479].

Asimismo la norma se encarga de regular las transferencias de estos datos entre países miembros de la Unión, por si durante el transcurso de una investigación penal, pueden ser de interés para varios de ellos. En la norma se regula el tratamiento de los archivos que contienen datos personales de cualquiera de los implicados en una investigación criminal, sin diferenciar entre ellos el rol que ocupan en la investigación: investigados, sospechosos, testigos, víctimas o terceros [480].

La finalidad de la Directiva es facilitar, agilizar y mejorar la transferencia de datos sobre una investigación, buscando así mejorar la prevención, la detección, la investigación, y el enjuiciamiento de actos penales, el cumplimiento de sanciones penales y la prevención de amenazas contra la seguridad pública[481].

El contenido de la Directiva no debe confundirse con las normas que regulan las actividades de cooperación judicial entre distintos Estados, que se rigen por sus propias normas[482], ya que el objetivo específico de esta última es el de proteger los datos recabados durante las investigaciones policiales [483], aunque se colabore con autoridades judiciales.

Se debe tratar de datos que, por su trascendencia, han de estar a disposición de órganos europeos de similares características a aquéllos que los han recabado, para que tengan conocimiento de ellos, y

---

[478] El Considerando 19 del Reglamento general sobre protección de datos dispone que "*La protección de las personas físicas en lo que respecta al tratamiento de datos de carácter personal por parte de las autoridades competentes a efectos de la prevención, investigación, detección o enjuiciamiento de infracciones penales o de la ejecución de sanciones penales, incluida la protección frente a las amenazas contra la seguridad pública y la libre circulación de estos datos y su prevención, es objeto de un acto jurídico específico a nivel de la Unión. El presente Reglamento no debe, por lo tanto, aplicarse a las actividades de tratamiento destinadas a tales fines. No obstante, los datos personales tratados por las autoridades públicas en aplicación del presente Reglamento deben, si se destinan a tales fines, regirse por un acto jurídico de la Unión más específico, concretamente la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo*".

[479] Considerando 12 y artículo 1.1 de la Directiva.

[480] Ver el considerando 30 y siguientes de la Directiva, que se centran en el principio de exactitud. En desarrollo de este principio, el art. 4.1.d) del cuerpo normativo, así como los arts. 6 y 7 son los que desarrollan el cumplimiento concreto de esta obligación.

[481] Considerando 4 de la Directiva en relación con el contenido del art. 1.2, apartados a) y b) del cuerpo de la norma.

[482] Considerando 5 de la Directiva.

[483] El Considerando 35 de la Directiva dispone que constituye su objeto sólo *«fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas para la seguridad pública. Entre tales actividades debe incluirse la protección de los intereses vitales del interesado"*. Sigue diciendo este Considerando que el derecho en que se concreta tal investigación cristaliza en la facultad atribuida a las autoridades para "*exigir u ordenar a las personas físicas que atiendan a las solicitudes que se les dirijan».*

hagan uso de la información obtenida, pero como datos especialmente protegidos[484]. En el caso de que los datos que se obtengan procedan del ámbito judicial[485] los órganos de cada nación competentes para tal proceso judicial (Jueces de Instrucción, Jueces de garantías, Fiscales), pese a la aplicación de las normas procesales, pueden adoptar también medidas para que los datos obtenidos queden incluidos en su ámbito de protección.

La Directiva otorga una importancia esencial al principio de exactitud, que se expresa en la obligación de mantener actualizados todos los datos procedentes de las investigaciones[486], lo que resulta trascendental ante su contenido y la finalidad que persigue. También se garantiza el derecho a la supresión de los datos[487], lo que también resulta importante precisamente por la naturaleza de estos.

La Directiva, en línea con la legislación general de protección de datos, sienta el principio de prohibición de recogida de datos sobre aspectos sensibles de la vida de las personas tales como la salud, la religión, la orientación sexual, el pensamiento político, etc. Paralelamente, excepciona este principio si otra norma europea o nacional prevé hacerlo con la finalidad de proteger a las personas, al interesado y éste haya hecho públicos tales datos[488]. Merece una consideración separada el tratamiento de datos que puedan tener alguna relación con derechos fundamentales de la persona afectada por el tratamiento de datos, en especial, se refiere la Directiva a los datos relativos al origen étnico[489], cuyo tratamiento se encuentra prohibido, salvo que existan adecuadas garantías de protección del interesado, la ley lo permita, o de su recopilación se derive la protección al interesado, o bien se trate de un dato conocido.

---

[484] Sirven para apuntalar estas afirmaciones el contenido de algunos considerandos. Así específicamente el número 7 y el número 12. Es especialmente significativo este último que ejemplifica diversas situaciones que implican actuaciones policiales, como por ejemplo disturbios públicos o grandes concentraciones como foco de recogida de datos de interés.

[485] El considerando 20 de la Directiva dispone que "«*La presente Directiva no impide que, en las normas nacionales relativas a los procesos penales, los Estados miembros especifiquen operaciones y procedimientos de tratamiento relativos al tratamiento de datos personales por parte de tribunales y otras autoridades judiciales, en particular en lo que respecta a los datos personales contenidos en resoluciones judiciales o en registros relacionados con procesos penales»*". También redunda en esta idea el considerando 80 del Reglamento, disponiendo que, aunque la protección de datos se extiende también a los recabados judicialmente, el ámbito de la Directiva no alcanza al ejercicio de la función jurisdiccional, ello con la finalidad de evitar cualquier forma de invadir la independencia del poder judicial.

[486] Considerando 30 de la Directiva en relación con el Art. 5.1.d del Reglamento, que lo recoge como principio.

[487] Art. 16.3.a).

[488] Art. 10.

[489] Considerando 37 de la Directiva. Hay que reseñar en este concreto apartado, el consentimiento del afectado al tratamiento de esta información puede ser tenido en consideración a la hora del tratamiento de estos datos de naturaleza tan sensible, pero no es fundamento jurídico único para hacerlo según la Directiva. Esto implica que el consentimiento por sí solo no basta para recopilar estos datos.

Entre su contenido, también destaca la regulación que reciben las operaciones de transferencias de datos entre organismos y Estados, lo que es básico para conseguir la finalidad de tener informados a los firmantes de las investigaciones y de los datos obtenidos[490].

En lo que se refiere a los datos en la nube, la Directiva no contiene ninguna regulación específica, porque es una regulación diseñada para poner en conocimiento de distintos países la existencia de investigaciones realizadas en otros Estados. En orden a cumplir esta finalidad, la transferencia de datos entre países, que es la finalidad propia de la Directiva, sólo podrá llevarse a cabo en situaciones en las que esos datos sean efectiva y realmente necesarios para quiénes los reclaman, y siempre para cumplir la finalidad perseguida por la norma, que es, en suma, la prevención, investigación y enjuiciamiento de delitos. Además, dichas transferencias deben hacerse entre dos o más entes que ostenten la condición de responsables de tratamientos de datos, con el fin de salvaguardar los derechos de los afectados[491].

Esta transmisión de datos no sólo puede hacerse entre países firmantes, sino que la Directiva contempla la posibilidad de que se haga también hacia países terceros. En este segundo supuesto, la Directiva, como ocurre también en la regulación del Reglamento antes analizado, exige que el estándar de protección, que reciban en su destino los datos que se envían, sea el mismo que tengan en su lugar de origen. En caso de que el nivel de protección que ofrece la entidad receptora no fuera el adecuado, se debe seguir un criterio de restricción en el envío, y supeditarlo a la protección y salvaguarda del afectado por esos datos, esto es, valorar si pese a la menor protección de los datos que se da el lugar en el que son reclamados, su envío puede ayudar a la persona sobre los que versan dichos datos[492].

Los derechos contenidos en la Directiva, así como los mecanismos de transmisión y demás aspectos contenidos en la norma, son sometidos a una autoridad de control que será la encargada de velar por el exacto cumplimiento de su contenido. Deben ser en todo caso entes independientes[493].

La tercera norma fundamental que guarda relación con la protección de datos en el ámbito europeo, y además con la investigación penal, es el Reglamento 2017/1939, de 12 de octubre de 2017, por el que se establece una cooperación reforzada para la creación de la Fiscalía Europea, ya que contiene obligaciones de protección de datos y de acceso a los mismos, pero también porque esta norma contiene algunas diligencias de investigación con las que se permite al Fiscal europeo investigar, y que pueden tener relación con los datos en la nube.

---

[490] Art. 35.
[491] Considerando 64 de la Directiva.
[492] Considerando 72 de la Directiva.
[493] Considerandos 75 a 79 de la Directiva.

Este nuevo Fiscal europeo, no es más que un organismo cuya finalidad es la investigación y persecución de *«delitos que perjudiquen a los intereses financieros de la Unión previstos en la Directiva (UE) 2017/1371 y determinados por el presente Reglamento, así como de ejercer la acción penal y solicitar la apertura de juicio contra sus autores y los cómplices de estos»*[494] y junto con estos delitos también puede investigar aquellos con los que pudieran estar «*indisociablemente vinculados»,* es decir los que guardan relación con la ejecución de éstos aunque no sean económicos.

Para cumplir con estas funciones, se atribuyen a este Fiscal europeo una serie de facultades expresadas en un amplio conjunto de diligencias de investigación, algunas relacionadas con el uso de los datos depositados en almacenamientos virtuales.

La sección segunda del Capítulo IV del Reglamento otorga al Fiscal europeo la facultad de inspeccionar un sistema informático y solicitar su bloqueo, a los efectos de evitar la pérdida de información; también puede solicitar la exhibición de datos informáticos (esta posibilidad está incluida en la facultad de solicitar que se le muestren documentos en cualquier formato), y más específicamente los almacenados y encriptados. También puede intervenir las comunicaciones del sospechoso o realizar seguimientos al investigado[495].

Por otra parte, valiéndose de nuestras normas procesales y de su facultad para *«inspeccionar… sistemas informáticos»*, puede instar que se acuerde por el Juez Instructor o por el órgano competente para ello en el caso de cada Estado, el registro de archivos contenidos en dispositivos incluso de modo remoto. Además, cuenta con la facultad para *«conseguir la presentación de cualquier dato informático almacenado, ya sean encriptados o descifrados, en su formato original o en otro formato determinado»,* e inmovilizarlos, puede exigir a cualquiera el dato almacenado en la nube.

En suma, cuenta con facultades para instar muchas diligencias distintas entre sí, pero la mayoría de las diligencias que puede solicitar están relacionadas con las nuevas tecnologías, llegándose incluso a aludir a que el trabajo de esta fiscalía será siempre en formato electrónico[496]. Se trata, pues, de una verdadera institución nacida y creada para el nuevo mundo tecnológico y digital.

Estas facultades de investigación, tan marcadas por el uso de las tecnologías, vienen reconocidas para que, mediante su uso, pueda cumplir mejor con la función que le ha sido atribuida de investigar hechos de trascendencia económica, en la que datos contables y financieros son esenciales, y donde

[494] Ver art. 4 del Reglamento 2017/1939.
[495] Este conjunto de facultades se enumeran en los apartados a hasta f del art. 30.
[496] Ver el considerando 47, que además hace alusión al empleo de sistemas de gestión de casos unificados a los efectos de tener constancia de las investigaciones llevadas a cabo.

muchos de ellos, por no decir la mayoría, suelen ser en la actualidad electrónicos. Por otro lado, la transnacionalidad de la ejecución del acto, y su importancia económica, necesitan de la intercomunicación de datos de la investigación lo que se facilita con el uso de soportes electrónicos de fácil transmisibilidad.

El Fiscal europeo cuenta con menos dificultades jurídicas para llevar a cabo estas diligencias de investigación electrónica, o al menos algunas de ella, que el Juez nacional español. Este último está obligado por sus propias competencias legales, circunscritas a las fronteras nacionales. Se ve necesitado de ayuda judicial internacional para acceder a la práctica de diligencias fuera de su territorio, lo que no le ocurre al fiscal europeo, cuyo ámbito abarca más de un país, y que puede acudir a la figura delegada en cada nación. El contenido de los artículos de la sección 1 del Capítulo IV, y en especial, el art. 23[497], relativo a las competencias territoriales de la Fiscalía Europea, le permiten pedir a cualquier empresa que aloje datos dentro del ámbito territorial de los países que suscriben su norma reguladora, la aportación de los datos radicados en la nube. Nuestras normas procesales, por el contrario, no son tan claras en este sentido, e incluso de serlo, no alcanzarían a países extranjeros.

El número de Estados que han suscrito el Reglamento[498] augura un importante alcance efectivo al desarrollo material de estas diligencias, si bien ha de matizarse esto, pues sólo podrá recabarse la información que esté en un servidor que esté dentro del territorio de alguno de los estados firmantes, quien habrá de haber legislado la realización de este tipo de diligencia, ya que depende de la legislación procesal nacional su articulación y la práctica concreta.

En el caso concreto de España, el Fiscal Europeo puede solicitar, por sí mismo o a través de los Fiscales delegados, haciendo uso de las normas procesales nacionales, que se acceda a un servidor ubicado en territorio español mediante la diligencia de registro remoto de equipos, o bien registrarlo mediante la diligencia de acceso a un dispositivo de almacenamiento masivo de información, que tales diligencias sean llevadas a cabo, lo que debe, en el caso particular de España, ser acordado por el Juez de Instrucción.

---

[497] Dispone dicho precepto en relación a la competencia territorial que: *«La Fiscalía Europea tendrá competencia respecto de los delitos a que se hace referencia en el artículo 22 cuando dichos delitos: a) hayan sido cometidos total o parcialmente en el territorio de uno o varios de los Estados miembros; b) hayan sido cometidos por un nacional de un Estado miembro, siempre que un Estado miembro sea competente respecto de ese tipo de delito cuando se haya cometido fuera de su territorio, o c) hayan sido cometidos fuera de los territorios a que se refiere la letra a) por una persona sujeta al Estatuto de los funcionarios o al Régimen aplicable a los otros agentes en el momento de la perpetración del delito, siempre que un Estado miembro sea competente respecto de ese tipo de delito cuando se haya cometido fuera de su territorio».*

[498] Según se desprende del propio tenor literal del Reglamento han sido *«Alemania, Bélgica, Bulgaria, Chipre, Croacia, Eslovaquia, Eslovenia, España, Finlandia, Francia, Grecia, Lituania, Luxemburgo, Portugal, República Checa y Rumanía».* En este sentido se indica que son estos países *«los que comunicaron el 3 de abril de 2017 al Parlamento Europeo, al Consejo y a la Comisión su deseo de establecer una cooperación reforzada sobre la base del proyecto de reglamento».*

En todo caso parece que la legislación sobre este particular en el ámbito de la UE resuelve mucho mejor la cuestión del registro de la nube, ubicada en distintos estados, que las normas nacionales, que resultan mucho más vagas e imprecisas acerca de la competencia territorial y la jurisdicción para realizar este tipo de diligencias.

La Fiscalía europea, en sus funciones de investigación, debe respetar la protección de los datos de las personas investigadas (tanto los datos personales de las personas físicas como titulares del derecho a la protección de sus datos, como los datos de las personas jurídicas en cuanto que constituyen un objeto de investigación que por sí mismo no debe divulgarse).

Dado que la investigación que realice dicha Fiscalía versará sobre el perjuicio que pudiera haberse causado a intereses financieros habrá un variado elenco de ilícitos penales susceptibles de ser instruidos: estafa, fraudes a Hacienda o la Seguridad Social o delitos societarios con implicaciones económicas, que reportará la obtención y uso de datos (contabilidades empresariales, declaraciones fiscales y a la seguridad social, relaciones de empleados, clientes, proveedores, pago de nóminas, facturas, saldos en cuentas corrientes o movimientos bancarios), lo que justifica el tratamiento de estos datos. Por eso puede comprenderse que a lo largo de la regulación de sus funciones aparezcan conceptos relacionados por ejemplo con investigaciones tecnológicas tales como elaboración de perfiles, seudonimización[499].

Las funciones de esta nueva Fiscalía están sometidas a control, y por ello, para llevar a cabo sus funciones y el uso de los datos, ha de actuar coordinadamente con el Supervisor Europeo de Protección de datos. Derivado de este uso de datos, y con escrupuloso respeto a los derechos derivados de los tratados fundacionales de las instituciones europeas, la Fiscalía está obligada informar al interesado de los datos que tengan sobre éste, lo que se puede limitar por los intereses de la investigación, así como por necesidades derivadas de la seguridad nacional o la salud nacional. En todo caso la exigencia de comunicación al interesado de los datos que se posean es algo novedoso[500], que ya hemos visto que se ha trasladado, en algunos casos muy concretos, a la legislación nacional.

En resumen, lo que puede destacarse de la regulación europea es que no hay una regulación expresa en materia de *Cloud Computing*. Las alusiones que hay sobre la operativa propia de estos servicios se refieren a transferencias de datos, que incluso no abarcan a los más íntimos o a los que pueden hacerse en el ámbito de la propia intimidad, lo que dificulta una posible localización (a salvo de que la autorización pudiera concretar el paradero de éstos), pero sin detallar el modo de acceso a los

[499] Ver el art. 2 del Reglamento 2017/1939.
[500] El Capítulo VIII, que comprende los arts. 47 a 89, son los que determinan el tratamiento de la información que se pone a disposición de la Fiscalía Europea.

mismos. Sólo se puede hablar de una alusión a una diligencia investigadora en el ámbito de las facultades de la Fiscalía Europea, la cual revestida de su ámbito trasnacional ve mejor resuelta las facultades de acceso a datos. En todo caso el ámbito territorial también está presente al verse circunscrita al ámbito de los países que han suscrito la creación de dicho organismo.

5.1.2.2. Las normas nacionales sobre protección de datos.

El marco legal español sobre la protección de los datos personales lo conforma actualmente la Ley Orgánica 3/2018, de Protección de datos personales y garantía de los derechos digitales, que deroga la Ley Orgánica de Protección de datos de carácter personal 15/1999, de 13 de diciembre[501]. Siguen vigentes el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal y la Ley 34/2002, de 11 de julio, de servicios, de la sociedad de la información y de comercio electrónico.

La Ley Orgánica 3/2018 adapta la legislación nacional al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de los datos de las personas físicas, el tratamiento de datos personales y la libre circulación de estos datos, y recoge además un conjunto de nuevos derechos ya existentes en la legislación comunitaria. El Real Decreto Ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos, resultó sólo una adaptación parcial a la legislación europea, referida únicamente a las infracciones y sanciones, y siendo aprobado por las Cortes y publicada en el BOE el día 15 de septiembre de 2018.

En el ámbito de la normativa nacional relativa a la protección de datos es también destacable el RDL 12/2018, de 7 de septiembre que regula la seguridad en las redes y en los sistemas de información.

La Ley de protección de datos derogada sí que definía el tratamiento de datos[502] como las «*operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias»*. La actual

[501] Agencia Española de Proteccion de Datos, *Guía para clientes que contraten servicios de Cloud Computing*. Madrid. 2013. Pág. 14. En la mencionada guía se señala especialmente el contenido de esta norma como la fundamental a los efectos de la protección de datos alojados en la nube, reseñando la obligación de los proveedores de esta clase de servicios de dar seguridad a los datos así almacenados.
[502] Texto del art. Art. 3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal.

ley que la sustituye no define en su articulado el tratamiento de datos, por lo que al ser su finalidad «*adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y completar sus disposiciones*», es en el Reglamento donde se encuentra dicha definición[503].

Pese a la amplitud de todas estas operaciones realizadas con datos personales, y que incluso algunas de estas acciones se pueden producir dentro de los servicios de alojamiento de datos en la nube, la ley española, como la normativa europea, tampoco regula esta actividad. La Ley Orgánica recoge aspectos que ya se contenían en la normativa anterior y reconoce y regula algunos nuevos derechos, y contiene disposiciones sobre la protección y seguridad de los datos[504].

En lo que se refiere a la prestación de servicios en la nube, como se ha dicho, son servicios que no se regulan en la Ley, que sólo se limita a reiterar que esta actividad conlleva el tratamiento de datos, porque cuando se lleva a cabo se recogen, conservan y modifican datos. Por lo tanto, las empresas que presten este tipo de servicios se someterán al contenido de esta ley al realizar procesos propios del tratamiento, siempre y cuando se den las condiciones de aplicabilidad del art. 2. apartado 1[505], quedando expresamente excluidas de su ámbito de aplicación aquellas actividades que, aunque tengan por objeto datos, queden excluidas del Reglamento europeo o bien se regulen por normativas específicas, como es, por ejemplo, la regulación aplicable a las actividades de investigación, prevención, enjuiciamiento y ejecución de infracciones penales.

Por otra parte, tal y como ocurre en el Reglamento 2016/679, el texto regula la transferencia de datos, que es la actividad que se realiza con datos que resulta más asimilable a la prestación de los

---

[503] Más en concreto en el art. 4.2 del Reglamento 2016/679, de 27 de abril, se define el «*tratamiento*» como «*cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;*».

[504] La protección principal que debe darse a los datos es conferirles seguridad desde un punto de vista técnico. La literatura sobre el particular, en concreto considera que las empresas del sector de la computación en la nube deben poder *«probar de algún modo que ha adoptado las cautelas previas necesarias para garantizar la seguridad en sus sistemas en sus dimensiones de integridad, confidencialidad y disponibilidad, y será capaz de responder ante cualquier incidencia de seguridad»* (Cfr. MARTÍNEZ MARTÍNEZ, RICARD. «El derecho y el Cloud computing» en MARTÍNEZ MARTÍNEZ RICARD (Editor), *Derecho y Cloud Computing.* Thomson Reuters-Aranzadi. Pamplona. 2012. Pág. 33).

[505] El precepto establece los supuestos en que el tenor literal de la norma le es aplicable a una entidad, fijando que es exigible su aplicación en los siguientes casos: *«a) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento. b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público. c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito».*

servicios en la nube. La regulación expresa de estas transferencias se desarrolla en los arts. 40 a 43 de la Ley, que se remiten al contenido del Reglamento europeo[506].

La conclusión que puede obtenerse del contenido de la regulación nacional sobre protección de datos y su relación con la investigación de los datos alojados en la nube, es muy similar, por no decir idéntica, que la que más arriba se expuso al hablar de las normas de la Unión Europea.

La Ley española, al tomar por remisión integra el contenido del Reglamento en lo que se refiere a los datos que están protegidos, excluye aquéllos que de forma personal gestiona el usuario en su actividad en redes sociales o correo electrónico. Por consiguiente, las normas específicas de transmisiones de datos a nivel internacional no son vinculantes para esta clase de actividades, lo que implica que la transferencia de datos de este tipo está fuera de cualquier clase de control.

La Ley Orgánica 3/2018, de 5 de diciembre tampoco contempla medidas especiales para los casos en el que los datos tengan relevancia penal, más allá de lo que dispone el art. 10 de la Ley. En este concreto precepto, la Ley Orgánica se remite, en el concreto caso de investigaciones judiciales, a las normas específicas sobre el particular, lo que nos llevaría nuevamente a necesidad de aplicar la Directiva 2016/680 que aún no ha sido traspuesta al ordenamiento jurídico nacional[507]. En suma, teniendo en cuenta esa ausencia de trasposición, cuando se trate de datos afectados por una investigación penal, la protección que se brinda a los mismos en la actualidad en España, es la que ofrece la escasa normativa existente de manera específica para tal fin, y que en la Ley Orgánica se remite al Reglamento 2016/679, que no regula la protección de datos en las concretas situaciones producidas en el seno de una investigación penal, y a la Ley Orgánica del Poder Judicial[508], que tampoco cuenta con disposiciones concretas sobre los datos relacionados con investigaciones criminales.

Es lógico concluir con que el tipo de datos que se puede recabar durante una instrucción penal, serán mayoritariamente los que se encuentren en alguno de los dispositivos personales encontrados durante la investigación. Igualmente puede ser común que este tipo de datos hayan sido depositados

[506] El Título VI de la Ley Orgánica 3/2018, de 5 de diciembre, recoge en los arts. 40 a 43 todas la regulación acerca de las transferencias internacionales de datos, así el art. 40 dispone que *«las transferencias internacionales de datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica y sus normas de desarrollo aprobadas por el Gobierno, y en las circulares de la Agencia Española de Protección de Datos. En todo caso se aplicarán a los tratamientos en que consista la propia transferencia las disposiciones contenidas en dichas normas, en particular las que regulan los principios de protección de datos"*. El resto de los preceptos regulan los mecanismos de autorización de tales transferencias internacionales de datos en los casos en los que esto resulte obligado, como cuando se trata de efectuar una de estas transferencias a países que según el regulador europeo no cuente con los márgenes de protección suficiente a los datos transferidos.

[507] Así se desprende expresamente de la lectura del artículo 1.3 de la Ley Orgánica, y del artículo 1.4 en su remisión a las normas reguladoras de determinadas instituciones como las penitenciarias, el Registro Civil, etc.

[508] La LOPJ contiene en sus arts. 236 bis a 236 nonies una regulación sobre la protección de los datos que se contienen en procesos judiciales y los que se manejan en la actividad propia de la oficina judicial y del Consejo General del Poder Judicial. Se trata de una regulación que no alcanza a los concretos tratamientos de datos derivados de procesos penales.

en una nube virtual bien por el investigado o bien por cualquier otro partícipe en los hechos delictivos. Ahora bien, teniendo en cuenta de que en la mayor parte de las ocasiones el origen, la transmisión y el uso de dichos datos será realizado dentro del ámbito de una gestión privada y personal, serán del tipo de datos cuya gestión por terceros queda excluida del ámbito de protección de las normas reguladoras de los datos personales. Ya se vio que el art. 2.2.c) del Reglamento 2016/679 excluía expresamente el tratamiento de datos que hace un particular en sus actividades personales o domesticas, y precisamente lo esperable de quien comete una infracción penal usando alguna clase de datos es que los genere, emplee y transmita, en la mayor parte de las ocasiones, amparado en la intimidad que brinda el ámbito doméstico. Este aspecto puede dificultar el acceso a los datos mediante el registro del dispositivo, ya que el contenido que se busca no estará en la memoria del aparato encontrado en buena parte de los casos, sino que el rastro de datos de tal acción se podrá encontrar bien en alguna red social o, en nuestro caso, en la nube. Pero el acceso a dicha nube se encuentra dificultado porque puede verse amparada la ausencia de tratamiento por terceros a los que pedir tales datos, en el hecho de que se trate de una actividad personal, privada y doméstica, con lo que la investigación debe continuar mediante otros medios. Por consiguiente, pese a que dichos datos se trasladen a otro servidor fuera del país, y pese a que los arts. 40 y siguientes de la Ley, regulen la transferencia de datos internacionales, esto no sirve para alcanzar el contenido de dichos datos, ni menos aún para controlarlos.

Este es el marco legal que sustenta parte de la actividad consistente en el suministro de los servicios en la nube que los particulares pueden emplear en España. Esta regulación, como puede verse admite que los datos que los particulares depositan en dichas nubes puedan salir fuera del territorio nacional, siempre y cuando se trate de datos de los que no tenga que darse cuenta a la hora de efectuar dicho traslado al exterior. En los casos en que dichos datos no sean de los que requieren dicha autorización, el traslado a servidores extranjeros no necesitará autorización por parte de los poderes públicos, lo que implicará que sea más fácil sacar esos datos, y como contrapartida, será más dificultoso que los mismos estén debidamente protegidos, y lo que es más importante a efectos de este trabajo, que sea posible localizar su destino y facilitar su acceso.

En todo caso, la existencia de un contrato entre el usuario y el suministrador para poder disfrutar de dichos servicios en la nube puede ayudar a obtener esos datos, cuando sean de utilidad para una investigación penal, solicitándolos directamente al suministrador. No obstante, esto es sólo una posibilidad, dado que normalmente los consentimientos recabados en este tipo de servicios pueden realizarse empleando un alias, o un nombre que puede ser tan imposible de encontrar como los datos que se desean localizar.

El hecho de que el servicio de nube se ejecute materialmente fuera de España [509], es decir, que los datos que se recaban en nuestro país terminen depositados en servidores fuera del mismo, requiere del consentimiento expreso al traslado de datos al contratar el servicio, porque de lo contrario éste no podría llevarse a cabo.

En todo caso este consentimiento se presta en el momento en el que se contrata el servicio, y la existencia de dicho contrato, de concurrir, podría constituir un medio válido para poder localizar los datos de interés para la investigación, pero debe dejarse claro que, si los datos no son de los que se tutelan mediante el Reglamento 2016/679 y la ley española sobre protección de datos personales, no les serán aplicables las normas sobre transferencia internacional de datos que contienen dichas normas y por consiguiente resultará más complejo localizarlos. A ello se suma el que tampoco ha sido objeto de trasposición la Directiva 2016/680 que regula el uso de los datos en las investigaciones penales, lo que podría ayudar a la hora de facilitar el acceso a este tipo de información.

La necesidad de tener que acceder al contenido de la información, en tanto que supone una actividad de tratamiento, se regula en la Ley, mediante la operación que el Reglamento denomina *«autenticación»*[510]*,* concepto que debe relacionarse con el de acceso autorizado, contraseña, control de acceso y copia de respaldo. La combinación de todos ellos permite vislumbrar el funcionamiento del servicio de alojamiento de datos en la nube[511]. La simpleza de la actividad encuentra un respaldo legal y consiste en que el usuario se autentica validando su usuario y su contraseña, de manera accede a los recursos y datos depositados en el servicio virtual, que son los que constituirían, en nuestro caso, el objeto de la investigación penal, y al que se llega mediante las diligencias descritas en distintos apartados de este trabajo.

En lo que se refiere a la aplicación de la Directiva 2016/680, que es la que específicamente regula los datos que se manejan en la investigación, prevención, enjuiciamiento y ejecución penal, cabe

---

[509] El art. 5.1.s) del RD 1720/2007 de 21 de diciembre que aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999 de 13 de diciembre ofrece una definición de lo que deba entenderse por *«Transferencia internacional de datos: Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español».*

[510] El apartado 2 del art. 5 del Reglamento aprobado mediante el RD 1720/2007 de 21 de diciembre que aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999 de 13 de diciembre, nos ofrece la definición.

[511] Dentro del apartado 2. letras a) hasta e) del art. 5 del Reglamento de desarrollo de la Ley Orgánica 15/1999 de 13 de diciembre, se define como *«Accesos autorizados: autorizaciones concedidas a un usuario para la utilización de los diversos recursos. En su caso, incluirán las autorizaciones o funciones que tenga atribuidas un usuario por delegación del responsable del fichero o tratamiento o del responsable de seguridad. b) Autenticación: procedimiento de comprobación de la identidad de un usuario. c) Contraseña: información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario o en el acceso a un recurso. d) Control de acceso: mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos. e) Copia de respaldo: copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación».*

recordar que no se encuentra traspuesta al ordenamiento español, porque lo que no constituye legislación nacional.

El contenido de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, completa a las normas nacionales anteriores, porque se refiere a la dimensión contractual del servicio electrónico, que en este caso es la prestación del servicio de alojamiento de datos, y otras funcionalidades, en la nube. Esta Ley parte de *«un concepto amplio de servicios de la sociedad de la información»,* que engloba «*....el suministro de información, servicios o aplicaciones facilitados por otros o a la provisión de instrumentos de búsqueda o de enlaces a otros sitios de Internet, así como cualquier otro servicio que se preste a petición individual de los usuarios (descarga de archivos de vídeo o audio...), siempre que represente una actividad económica para el prestador. Estos servicios son ofrecidos por los operadores de telecomunicaciones, los proveedores de acceso a Internet, los portales, los motores de búsqueda o cualquier otro sujeto que disponga de un sitio en Internet a través del que realice alguna de las actividades indicadas, incluido el comercio electrónico»*[512].

En lo que se refiere al lugar desde el que estas empresas prestan los servicios se diferencia, de un lado, las entidades que prestan servicios electrónicos en España contando con domicilio social en España, y por consiguiente es en nuestro país donde la compañía cuenta con la dirección y el control, y de otro lado, las empresas que sólo tienen un establecimiento permanente en España.

En el primer caso es íntegramente aplicable la legislación nacional, y en el segundo caso la aplicación de la ley es simplemente parcial[513]. Este extremo, muy vinculado a la territorialidad, también tiene implicaciones procesales sobre todo a la hora de saber a qué entidad hay que dirigirse, y dónde se encuentra, a la hora de solicitar datos. La aplicación más o menos extensa de la ley, derivada de la mayor o menor implantación de la compañía en territorio nacional, es la que determina «*las obligaciones y responsabilidades de los prestadores de servicios que realicen actividades de intermediación como las de transmisión, copia, alojamiento y localización de datos en la red»*[514].

Entre estas obligaciones las hay tan genéricas como las que consisten en *«un deber de colaboración para impedir que determinados servicios o contenidos ilícitos se sigan divulgando»*, pese a lo que

[512] Exposición de motivos, apartado II de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
[513] Los arts. 2, 3 y 4 de la Ley 34/2002, de 11 de julio, diferencian entre Prestadores de servicios establecidos en España de los establecidos en otro Estado miembro de la Unión Europea o del Espacio Económico Europeo. Considera que están establecidos en España quien tiene su sede social en el país, o bien quien tiene alguna clase de establecimiento en el mismo. La mera tenencia de instalaciones tecnológicas no sirve para exigir la observancia de la ley.
[514] Exposición de motivos, apartado III de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

se su inobservancia comporta consecuencias no sólo «*de orden administrativo, sino de tipo civil o penal, según los bienes jurídicos afectados y las normas que resulten aplicables*»[515].

Lo anterior permite concluir con el hecho de que las entidades que ofertan en España servicios en la nube no están sujetas a más requisitos, que los propiamente jurídico-mercantiles habituales, y a las prescripciones de las leyes de protección de datos que han sido esbozadas en este apartado. La Ley fija un principio de libertad de prestación de servicios y de no sujeción a autorización[516], permitiendo sólo restricciones en los casos de *«la investigación penal»*, o supuestos de vigilancia recíproca que impidan las conductas vulneradoras de derechos[517]. Estas conductas que tienden a evitar dichas vulneraciones se concretan en la obligación que se impone a estas entidades dedicadas a trabajar en el tratamiento de datos para que entreguen los datos del responsable de un servicio de la sociedad de la información[518], mediante autorización judicial, que permita identificarlo y localizarlo, y con ello evitar que realice una conducta contraria a las disposiciones legales. En caso de que sea un prestador de servicios intracomunitario, han de seguirse las normas de cooperación expresamente previstas en la Ley.

En orden a proteger los datos, la Ley faculta a los órganos judiciales para recabar *«la autorización del secuestro de páginas de Internet o de su restricción cuando ésta afecte a los derechos y libertades de expresión e información y demás amparados en los términos establecidos en el artículo 20 de la Constitución»*[519]. Es decir, se deja a la autoridad judicial la medida estrictamente limitadora de concretos derechos fundamentales como la libertad de expresión o LA libertad de información, sin que se enumeren en ningún caso los contemplados en el art. 18 CE, cuya protección penal es parte del objeto de estudio de este trabajo.

Por otro lado, y también relacionado con la responsabilidad de las empresas prestadoras de servicios de alojamiento de datos[520], se les exonera por aquellos datos de contenido ilegal que alojen sus

---

[515] Exposición de motivos, apartado III de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

[516] Arts. 6 y 7 de la Ley 34/2002, de 11 de julio.

[517] En el art. 8.1 de la Ley 34/2002, de 11 de julio, se reflejan como criterios de especial protección *«a) La salvaguarda del orden público, la investigación penal, la seguridad pública y la defensa nacional; b) La protección de la salud pública o de las personas físicas o jurídicas que tengan la condición de consumidores o usuarios, incluso cuando actúen como inversores; c) El respeto a la dignidad de la persona y al principio de no discriminación por motivos de raza, sexo, religión, opinión, nacionalidad, discapacidad o cualquier otra circunstancia personal o social, y d) La protección de la juventud y de la infancia; e) La salvaguarda de los derechos de propiedad intelectual»*.

[518] Art. 8 de la Ley 34/2002, de 11 de julio.

[519] Art. 11.3 de la Ley 34/2002, de 11 de julio, introducido por la Ley 56/2007, de 28 de diciembre, de impulso de la sociedad de la información.

[520] El art. 16 de la Ley 34/2002, de 11 de julio, expresamente dispone que: *«1. Los prestadores de un servicio de intermediación consistente en albergar datos proporcionados por el destinatario de este servicio no serán responsables por la información almacenada a petición del destinatario, siempre que: a) No tengan conocimiento efectivo de que la actividad o la información almacenada es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o b) Si lo tienen, actúen con diligencia para retirar los datos o hacer imposible el acceso a ellos. Se*

clientes, salvo que los hubiesen conocido con anterioridad a ser alojados, o actuasen en nombre y por cuenta de la empresa alojadora. Es una medida coherente porque el prestador no debe ni puede conocer el contenido de los datos alojado usando el servicio, pues lo contrario es una vulneración del derecho a la protección de los datos personales[521].

Esto último se vincula con lo que ya se ha dicho con relación a la exclusión del ámbito de protección de las normas protectoras de los datos personales cuando son los propios ciudadanos quienes tratan dichos datos dentro de su ámbito personal o doméstico. Precisamente el hecho de que la Ley recuerde este aspecto, refuerza la idea que se ha ido sosteniendo al amparo de la disposición contenida en el art. 2.2 c) del Reglamento; esto es, que al excluirse del ámbito de la protección del derecho a los datos personales, aquellos tratamientos realizado en el ámbito personal por el titular de tales datos, las empresas que ofrecen estos servicios (soporte de redes sociales, o nubes virtuales) no deben ser responsables de los contenidos de tales datos, incluyendo, por supuesto, los de contenido penal.

La ausencia de una regulación especializada sobre las empresas de servicios en la nube, unida a la extraordinaria facilidad para que los datos que sean de naturaleza personal se excluyan de todo control a la hora de ser transferidos fuera de fronteras nacionales, constituyen un hándicap a la hora de poder acceder a dichos datos y para analizarlos, cuando éstos puedan ser de interés para una investigación penal. Es decir, que, pese a que se cuenta con una herramienta procesal, que expresamente admite la posibilidad de acceder y analizar los datos contenidos en repositorios virtuales, existirá una clara dificultad para saber dónde están esos datos, bajo qué empresa o entidad vienen siendo albergados mediante un servicio contratado en la nube, y por consiguiente llegar hasta ellos. Todo esto puede redundar en el modo en que la medida de investigación consistente en el registro de los datos se ejecute, y en el hecho mismo de que pueda llevarse a cabo.

5.2. Los datos electrónicos: regulación legal y su consideración como objeto de intervención.

---

entenderá que el prestador de servicios tiene el conocimiento efectivo a que se refiere el párrafo a) cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse. 2. La exención de responsabilidad establecida en el apartado 1 no operará en el supuesto de que el destinatario del servicio actúe bajo la dirección, autoridad o control de su prestador».

[521] Incluso podría comportar la realización de alguna clase de ilícito penal que pudiera vulnerar el derecho a no divulgar datos, secretos o comunicaciones.

La lectura de los dos apartados anteriores permite llegar a la conclusión de que en la actualidad, y pese a lo reciente de todas las normas reguladoras acerca de la protección de datos, no existe una regulación específica sobre el *cloud computing*, y ello a pesar de la intensa relación que guarda esta ultima actividad con aquéllos. No obstante, a pesar de esto, algunos preceptos legales de normas que regulan aspectos de la protección de datos, sin llegar a normativizar dicha actividad por completo, sí que tratan concretos aspectos parciales de tal actividad, especialmente en materia de la transmisión de datos, que no deja de ser parte integrante del alojamiento de datos en la nube.

En todo caso, lo que ahora procede analizar es la regulación existente sobre la protección de los datos electrónicos. Esto resulta especialmente importante en el caso de las diligencias de investigación electrónica, en la que son los datos electrónicos son el objeto de búsqueda y análisis a efectos penales.

En primer lugar, y una vez sentada la perspectiva procesal penal desde la que se analiza el concepto de dato electrónico, puede decirse que los datos, a los efectos procesales que se estudian en esta tesis, vienen constituidos por cualquier información o conocimiento inicial sobre alguna materia que se materializa en formato electrónico[522]. A su vez, la importancia del formato electrónico de los datos es incluso recogida por parte del Diccionario de la Lengua, que entre las varias acepciones que ofrece del concepto de dato, comienza calificándolos como aquella *«información sobre algo concreto que permite su conocimiento exacto o sirve para deducir las consecuencias derivadas de un hecho»* [523], llegando a ofrecer un concepto más aproximado al dato informático o electrónico, en su tercera entrada, cuando indica que es la *«información dispuesta de manera adecuada para su tratamiento por una computadora»* [524]. De esta definición se desprenden dos características esenciales del dato informático: que se genera mediante un instrumento electrónico y que se trata de un elemento objeto de tratamiento.

En el ámbito estrictamente procesal penal, y en la instrucción criminal, se atiende a los datos por su contenido, su ubicación o por su importancia a la hora de hacer avanzar la investigación, o por todos estos criterios conjuntamente considerados. Por ello dentro del ámbito de la investigación penal no sirve clasificar los datos atendiendo a los criterios de las leyes que regulan la protección de datos o el comercio de dichos datos. Esto se debe a que las investigaciones de esta naturaleza no se

[522] Cfr. DAVARA RODRÍGUEZ, Miguel Ángel. *Manual de derecho informático.* 11ª ed. (rev. y puesta al día). Cizur Menor Aranzadi, Navarra 2015. El autor en el segundo capítulo de la obra dedicada a la protección de datos, describe en el apartado de generalidades una definición básica de dato, indicando que: *«entendemos por dato el antecedente o noticia cierta que sirve de punto de partida para la investigación de la verdad».* Se ha utilizado la modalidad de recurso electrónico que no se encuentra paginada, por eso no se ha podido señalar la página exacta.
[523] Diccionario digital de la Real Academia Española. Ver enlace: http://dle.rae.es/srv/fetch?id=Bskzsq5|BsnXzV1.
[524] Tomado de la definición que se ofrece del sustantivo dato en el diccionario de la Real Academia española, en su versión virtual. Enlace web: https://dle.rae.es/?id=Bskzsq5|BsnXzV1

rigen por la mayor o menor protección de los datos electrónicos, o si el contenido de éstos puede considerarse como personal o no, sino que todos los datos electrónicos, sin excepción, pueden ser traídos al proceso, porque todos pueden servir para acreditar un hecho y con ello cumplir con la finalidad investigadora perseguida.

El verdadero objeto de interés en la instrucción penal es el contenido alojado en instrumentos tecnológicos de cualquier clase y, en algunas ocasiones, la actividad consistente en crearlos y generarlos. Por lo tanto, es más relevante para la regulación procesal las funciones del dispositivo: receptora, generadora y vehicular, que el dato por sí sólo, o su grado de protección. De lo que se trata es de obtener información relevante[525], no de detenerse en el tipo de dato del que se trata, pues en atendiendo a esta última categoría, lo que ha de servir de interés es la relación de dicho dato con la afectación de alguno de los derechos enunciados en el art. 18 CE, y si existe alguna clase de limitación a alguno o a varios de dichos derechos, será el auto judicial el que pondere la necesidad de traer esos datos a la instrucción. En este acto de valoración no se va a atender al tipo de dato, sino a su relación con los hechos investigados y a valorar si tal interés compensa limitar el derecho constitucional que protege dichos datos.

Las tres funcionalidades de los dispositivos electrónicos que se han mencionado, receptora generadora y vehicular, se desprenden del contenido de la regulación de las diligencias de investigación.

En concreto, en la diligencia de registro de dispositivos de "almacenamiento masivo de información", la función de depósito, recipiente, acopio, o bien simplemente la función propiamente acumuladora de datos parece destacarse incluso desde su denominación, porque de lo que se trata es de obtener del recipiente encontrado los datos que pudieran alojarse en el mismo.

El rasgo que define al dispositivo es el de servir para guardar datos. El art. 588 sexies a1, y el art. 588 septies a1 LECrim son los preceptos que enumeran los dispositivos que sirven para esta función, admitiendo incluso a los virtuales. La ley también considera como receptáculo de información incluso a *«un sistema informático o parte del mismo*». El dispositivo que la ley

[525] Cfr. DAVARA RODRÍGUEZ. Manual de derecho informático. Op. Cit. Capítulo II, La protección de datos, apartado 2, Datos, información e informática. Se ha utilizado la modalidad de recurso electrónico que no se encuentra paginada El autor diferencia las categorías de dato y de información. textualmente pone de manifiesto que *«Esto es, mientras el dato no resuelva una consulta determinada, no sirva a un fin, no dé respuesta o no oriente la posible solución a un problema, es el antecedente o punto de partida para la investigación de la verdad; pero, en el momento en que ese mismo dato da respuesta a una consulta determinada, o sirve a un fin, o se utiliza para orientar la solución a un problema, se ha convertido en información».* El autor aprecia en el dato un prius, es decir un aspecto que indica que no ha sido reformado o sometido a tratamiento alguno, y que una vez que lo ha sido, puede obtenerse del dato originario verdadera información.

considera susceptible de registro es todo aquel que sirve para contener datos: un ordenador, un GPS, un smartphone, la nube, la intranet de una empresa[526], o cualquier otro similar.

La legislación además de la función de depósito o recipiendaria admite una función creadora tanto de información como de datos. Del mismo modo que pasaba con la función anterior, no importa el tipo de dispositivo, sino esta vez, lo que se destaca para que concurra esta función, es la cualidad del aparato para generar y crear datos. Esta función creadora de datos del dispositivo es la que predomina sobre todo en la diligencia de registro remoto. Nuevamente, como en la función anterior, la finalidad de la intervención es la de acceder y analizar los datos, que aportan conocimiento de los hechos investigados. En cambio, en el caso concreto de esta diligencia de registro remoto la cualidad de la información reside, sobre todo, en que estos datos se generan de forma dinámica, creándose los archivos en ese momento, intercambiándose, enviándose o recibiéndose, sin perjuicio de que, además, también pueda interesar un dato concreto que ya estuviera almacenado. Pero, cabe insistir, en que la finalidad de un registro remoto no reside tanto en encontrar lo que podría obtenerse mediante una entrada y registro en domicilio y la requisa del ordenador, como analizar la creación de datos on line.

La tercera función es la vehicular, y en ella es el dispositivo el que se concibe como medio para acceder a la información. Se trata de una función que es predicable de las diligencias de investigación electrónica que son objeto de análisis particular en esta tesis, porque en ambas es posible usar los dispositivos como medio de acceso a la información alojada virtualmente.

En cualquiera de las tres funciones, y con independencia de la actividad que el dispositivo pudiera ejercer sobre los datos, éstos, siempre que su contenido pudiera afectar a derechos del art. 18 CE, deben ser extraídos y analizados mediante una autorización judicial.

En realidad, desde un punto de vista material, los datos no son más impulsos eléctricos transformados en información. Desde este punto de vista técnico, es indiferente que gocen de mayor o menor protección desde el punto de vista de la ley de protección de datos o cualquier otra norma

[526] Cfr. VIZÁN PÉREZ, Esther. Transmisión de información por medios convencionales e informáticos: operaciones de grabación y tratamiento de datos y documentos (ADGG0508), Editorial CEP, S.L., 2014. Pág. 80. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/bupo-ebooks/detail.action?docID=4508023. La autora realiza una muy precisa definición de este concepto indicando que «*Intranet: es una red informática que utiliza el protocolo de Internet para poder compartir servicios de información. El objetivo de la Intranet es ahorrar costes, ganar en eficiencia y ser más competitivos. La intranet está muy extendida en las empresas. Nos facilita el funcionamiento entre grupos, videoconferencias, ventas, gestión de clientes, gestión de proveedores, productividad. También se utiliza para la cultura corporativa de las empresas. La intranet está en un ordenador que se le denomina servidor en el cual tenemos alojado una página web (intranet). Mediante un ordenador portátil o el ordenador de sobremesa podemos abrir la página web donde se encuentra alojada esa intranet y mediante un usuario y contraseña accederemos a ella*». Tal y como podemos concluir al estar los datos que son objeto de estudio fuera del ordenador que se emplea para trabajar sobre ellos puede apreciarse que el dispositivo es intangible en tanto que los datos finalmente depositados en ello pueden estar muy alejados del lugar desde el que se accede a los mismos.

general o especial o procesal penal. Por el contrario, al proceso penal le interesa la información en la que se transformas esos impulsos eléctricos, resultándole de especial interés su contenido. No obstante, además del contenido, puede ser de interés para la investigación el paradero o la ubicación de estos datos, porque cabe plantear en hipótesis que durante la instrucción, la búsqueda de los datos de interés para la investigación, conduzca hasta entidades que prestan servicios en la nube en cualquiera de las tipologías existentes (hosting o housing[527] o alojamiento de información[528]), y dicho paradero puede determinar un modo concreto de acceso hasta ellos, diferenciado en función de su localización. En este sentido, el dato es un objeto de la investigación que ha de incorporarse a las actuaciones cumpliendo con todos los presupuestos y requisitos legales, entre los que están la necesidad de que se investiguen por una jurisdicción estatal competente[529] la concurrencia de los demás indicios de comisión de ilícitos penales.

5.2.1. Concepto jurídico de dato.

El concepto de dato, además de abarcar un objeto de estudio para el proceso penal, es también jurídico. La regulación de los datos en España se contiene en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, que tiene por objeto regular el contenido del art. 18.4 de la Constitución. Esta ley, que protege los datos personales, no nos ofrece una definición de dato, que, en cambio, sí que se contenía en la norma derogada. La Ley derogada definía el dato como «*cualquier información concerniente a personas*

[527] La diferencia entre ambos conceptos deriva del alquiler de equipos. Así estaremos ante el posting cuando la empresa alquila los equipos en que se guardan los datos, mientras que en el housing no sucede así, sino que lo que se oferta es una ubicación para los datos. La distinción la realiza Vid. MARTINEZ MARTINEZ, RICARD. «El Derecho y el *Cloud computing*» en MARTíNEZ MARTíNEZ RICARD (Editor), *Derecho y Cloud Computing.* Thomson Reuters- Aranzadi. Pamplona. 2012. Pág. 23.

[528] Cabe citar a título de ejemplo por ser sobradamente conocidas el servicio dropbox de Microsoft, o el servicio de icloud de Apple, entre otros muchos operadores que ofertan en el mercado esta clase de servicios, a veces de modo completamente gratuito. Pero también se ofrecen servicios de hosting no solo para particulares sino también para empresas. Se puede consultar en cualquier página web especializada la enorme variedad de entidades, además de las más conocidas que realizan estas actividades: https://www.revistacloudcomputing.com/2012/01/directorio-de-empresas-de-cloud-hosting-en-espana/. El listado que contiene se refiere a las siguientes: Arsys (http://www.arsys.es/cloud-hosting); AZAMedia(http://www.azamedia.com/cloud-hosting); Clarinet (http://www.claranet.es/cloud-hosting); Comalis (http://www.comalis.com/cloud); Dinahosting (https://dinahosting.com/cloud-hosting); Gigas (http://gigas.com); Ilimit Comunicacions (http://www.ilimit.com/es/cloud-hosting); Interdominios, (http://www.interdominios.com/cloud-computing); Interhost (http://www.interhost.com/es/cloud-hosting): Neodigit (http://www.neodigit.es/cloud-hosting); Occentus Network (http://www.occentus.net/hosting); Ran Networks (http://www.ran.es/cloud-computing); 1&1 (http://alta.1and1.es/CloudDynamicServer).

[529] Los problemas derivados de la ubicación de los datos y la posible afectación de la competencia territorial del juez no es una cuestión nueva, ya antes de la versión final de la reforma de la LECrim en 2015, y durante el desarrollo del Proyecto de Código Procesal Penal, fue un asunto sobre el que la doctrina se interrogó. Vid. ORTIZ PRADILLO, Juan Carlos. *Problemas procesales de la ciberdelincuencia*. Colex. Madrid. 2013. Pág. 196.

físicas identificadas o identificables»[530]. En la actualidad, pese a la ausencia de definición expresa de nuestra Ley, puede encontrarse un concepto normativo en el Reglamento 2016/679 de 27 de abril, que sí que la aporta, y cuyo contenido no varía con respecto al anterior, estimando que un dato es aquello que permite a alguien ser identificado o poder ser identificable[531].

En el caso de la investigación criminal, los conceptos que emplea la legislación sobre la protección de datos personales resultan difusos e inconcretos. Por lo demás realizar una definición de datos por parte de esta norma y a efectos penales es innecesario, porque para tal investigación penal, lo relevante no es que el dato deba entenderse conforme a sus leyes protectoras, sino el contenido que dichos datos aportan al proceso. Para el juez instructor no importa que el dato sea de naturaleza personal o no lo sea, lo que le interesa es si el acceso a ese dato, por ser su contenido útil para la instrucción, conlleva o no limitar derechos fundamentales de los del art. 18 CE, porque, en el caso de que se limiten de alguna manera, se exige un pronunciamiento judicial que valore la limitación de dichos derechos, puestos en relación con los hechos que están bajo investigación; por el contrario, si no se limita ningún derecho fundamental, esa resolución judicial no es necesaria y puede incorporarse a las actuaciones sin la intervención judicial que se exigiría en el caso anterior.

Las leyes sobre protección de datos tienden a regular concretos aspectos parciales de los datos de las personas físicas, relacionados principalmente con el ejercicio de una actividad mercantil ejecutada por terceros, que son los que usan estos datos como objeto de su actividad. Estas normas regulan el uso y tratamiento de datos personales en el sector de las comunicaciones y los servicios electrónicos en general, y desde esta óptica es cómo el legislador pone límites al uso que se puede hacer de ellos. En cambio, cuando se habla en estas leyes de la investigación criminal, es para poner de manifiesto que los datos que están en poder de los distintos operadores deben ser conservados y entregarse siempre que lo pidan los jueces de instrucción[532].

En esta finalidad de custodia y preservación, la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, impone a los prestadores de este tipo de servicios la obligación de conservar los *«datos generados o*

---

[530] Art. 3, apartado a) de la Ley Orgánica derogada.

[531] A tales efectos, el apartado 1 del art. 4 del Reglamento 2016/679, "*considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;"*

[532] El art. 1.1 de la Ley 25/2007, de 18 de octubre determina que: *«1. Esta Ley tiene por objeto la regulación de la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de dichos datos a los agentes facultados siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales.»*

tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación», y más concretamente, *«los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o usuario registrado»*[533]. Dado que pueden afectar a una investigación criminal, se regula la cesión de estos datos a los agentes facultados judicialmente con la finalidad de investigarlos.

Esta obligación que se impone a los prestadores deriva de su actividad consistente en prestar «*servicios de comunicaciones electrónicas o de redes públicas de comunicación»*, que generan datos electrónicos que deben ser conservados y protegidos. De la obligación general se desglosan otras como la de conservar los «*datos de tráfico y de localización sobre personas físicas y jurídicas»*, pero excluyendo «*...el contenido de las comunicaciones electrónicas, incluida la información consultada utilizando dicha red»*.

El art. 3 enumera exhaustivamente los tipos de datos que deben conservarse por haber sido generados en un acto de comunicación lo que aporta una idea de la información que debe ser objeto de preservación a tales fines[534]. No obstante, se debe tener en cuenta, que esta cuestión es polémica, y aunque el tenor de la Ley 25/2007 sigue en vigor, la jurisprudencia del TJUE ya determinó que no resultaba posible un almacenamiento masivo e indeterminado de información de los usuarios siempre que ello no viniera exigido y motivado ante una situación concreta, eliminando con ello la posibilidad de almacenamientos generalizados de datos que más tarde, en caso de ser necesario, se cedían a las investigaciones penales que lo requiriesen[535], pues *«la retención y conservación generalizada e indiscriminada de estos datos de tráfico y localización resulta contraria a los derechos fundamentales de los ciudadanos reconocido en la Carta Europea de Derechos Humanos»*[536].

La misma idea de custodia y mantenimiento de la información subyace, para el caso de las intervenciones de comunicaciones en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, que permite interceptar «*cualquier comunicación que tenga como origen o*

---

[533] Ambas cursivas están tomadas del contenido del art. 1, apartados 1 y 2 de la Ley 25/2007.

[534] En todo caso la entrada en vigor de la nueva normativa europea deja tocada a juicio de la doctrina el contenido de esta ley. Vid. BALLESTEROS MOFFA, Luis Ángel. «La difícil situación de la Ley 25/2007 de conservación y cesión de datos de tráfico y localización en las comunicaciones electrónicas: la «tala» de su base comunitaria y los desfavorables vientos desde sus homólogas europeas». *Revista Aranzadi de Derecho y Nuevas Tecnologías* núm. 44/2017 parte Estudios jurídicos. 2017. BIB 2017\12592. Págs. 4 y 5.

[535] Se trata de la STJUE (Gran Sala) de 21 de diciembre de 2016. La sentencia y sus consecuencias son analizadas en COLOMER HERNÁNDEZ, Ignacio «Uso y cesión de datos de las comunicaciones electrónicas para investigar delitos tras la STJUE de 21 de diciembre de 2016», en RUDA GONZÁLEZ, Albert (Coord) y JEREZ DELGADO, Carmen (Coord), *Estudios sobre Jurisprudencia Europea. Materiales del I y II encuentro anual del Centro español del European Law Institute*. Ed. Sepin. Madrid. 2018. Págs. 767-781. El autor sostiene que la consecuencia derivada de dicha sentencia es que la acumulación de datos de trafico de manera genérica *«no pueden ser cedidos por orden judicial para investigar los delitos al amparo de la previsión contenida en el art. 588 ter. J. LECrim»*

[536] COLOMER HERNÁNDEZ, Ignacio, Op. Cit. Pág. 768.

destino el punto de terminación de red o el terminal específico que se determine a partir de la orden de interceptación legal, incluso aunque esté destinada a dispositivo de almacenamiento o procesamiento de la información». En este caso, la comunicación sólo se podrá intervenir ante la existencia de una orden judicial, y el deber de conservación de los datos que se impone a los prestadores del servicio, se ciñe a los que se generan por el uso de la red que genera un cúmulo de datos que obligatoriamente deben ser retenidos. Se trata pues del deber de conservar los datos que se generan por el uso de la red.

La Ley descarta cualquier clase de excepción a este deber de conservación, extendiendo esta obligación a los datos que se generen por la realización de «*todo tipo de comunicaciones electrónicas….que se realicen mediante cualquier modalidad de los servicios de telefonía y de transmisión de datos, se trate de comunicaciones de vídeo, audio, intercambio de mensajes, ficheros o de la transmisión de facsímiles. El acceso facilitado servirá tanto para la supervisión como para la transmisión a los centros de recepción de las interceptaciones de la comunicación electrónica interceptada y la información relativa a la interceptación, y permitirá obtener la señal con la que se realiza la comunicación»* [537].

El carácter general de la conceptuación de los datos electrónicos, es decir, la importancia de estos para el proceso penal derivado de su contenido y no de su tipología, también se deduce de la propia LECrim. Los arts. 588 bis y siguientes de la LECrim, pese a que regulan los aspectos comunes a todas las diligencias de investigación electrónica, no definen lo que es un dato, y mucho menos los categorizan. La ley procesal parte de un concepto de dato omnicomprensivo, considerando como tal a todo elemento electrónico ubicado dentro de un dispositivo (cuyo concepto también es muy amplio) que puede ser intervenido, analizado y depositado como parte del proceso. Hay varias reiteraciones de esta omnicomprensividad, por ejemplo, en el art. 588 ter, apartado d) LECrim, según el cual se puede pedir, sin limitación alguna, *«el conocimiento de otros datos de tráfico asociados o no asociados pero de valor añadido a la comunicación».*

El legislador procesal no podía dar una respuesta diferente ante los diferentes tipos de datos que existen en la actualidad, porque no se puede constreñir la investigación penal con un concepto restrictivo del dato como objeto de análisis, al contrario, a tales fines, el concepto de dato debe ser lo más amplio posible.

La finalidad que persigue el legislador es la de permitir el buen fin de la investigación, y habilitar los medios legales que permitan conseguir todos los datos que sean necesarios para eso, con independencia de su contenido y de la categoría legal a la que puedan pertenecer; pues la

[537] Art. 33 de la Ley 32/2003, de 3 de noviembre, general de telecomunicaciones.

instrucción requiere el cotejo e interpretación de todos los que guarden interés con los hechos investigados, y limitar su contenido acudiendo a la tipología que sea, sería contraproducente para el examen jurídico de los hechos.

Esta misma amplitud en el modo de entender los datos también se extiende a los obligados a entregarlos a las autoridades [538], lo que refuerza la idea ya aludida, de que lo importante es alcanzar el resultado previsto en la instrucción, imponiendo para ello las obligaciones de entrega a quien fuera menester.

En cambio, esta amplitud no puede predicarse en materia de ubicación de los datos. Así, el legislador, que salva la tipología de datos con la obligación de obtener resolución judicial o impone, a cualquier agente del tráfico comercial relacionado con los datos, la obligación de entregarlos, no se ha ocupado con la misma amplitud de regular lo que se refiere al lugar en que se encuentran los datos, sin tener en cuenta que el lugar de ubicación de los mismos puede determinar diferentes regímenes en orden a las obligaciones de entrega y de conservación de los datos.

En lo que se refiere a la ubicación material de los datos la Ley parte de las ideas expresadas en el Convenio sobre ciberdelincuencia, que ya fue objeto de análisis. Según el criterio sentado en una parte de dicho instrumento sólo se pueden acceder y registrar los datos que están dentro del territorio de aquel país que ordena tal examen. El Convenio de Budapest es muy claro en esta cuestión. En cambio, el legislador español, aunque ha sido fiel a esta premisa, ha abierto el abanico de posibilidades de registro más allá de las fronteras nacionales, aunque sólo circunscrito a los datos alojados en servicios en la nube, y de un modo un tanto confuso[539].

En todo caso, y como resumen a lo dicho hasta el momento, cabe señalar que el concepto de dato para la legislación procesal no está anclado a aspectos técnicos que constriñan el objeto de búsqueda y de investigación. Es un concepto buscadamente amplio, que permite acceder a cualquier dato que arroje información, sin limitación alguna derivada de su clasificación legal, y sólo y únicamente siempre que guarde relación con los hechos objeto de la investigación, y afecte su

[538] A título de ejemplo el contenido general del artículo 588 ter, apartado e de la LEcrim es suficientemente significativo de esta obligación de colaboración genérica impuesta a terceros, y que de forma detallada hemos deslindado en las diligencias de acceso a dispositivos de almacenamiento masivo de información y en la consistente en la de acceso remoto a equipos informáticos, pero que de forma resumida se puede concretar empleando el tenor del texto legal en el deber de colaboración que se impone a *«todos los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, así como toda persona que de cualquier modo contribuya a facilitar las comunicaciones a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual».* Como puede verse el legislador trata de llegar a todos aquellos que están implicados de una u otra forma en los mecanismos de comunicación en concreto, o en servicios electrónicos en general.

[539] En este aspecto me remito al apartado 2.2.3 de esta tesis en la que se estudia el acceso a repositorios de datos y se analiza el contenido del texto legal, así como sus problemas concretos.

acceso o su registro al contenido de alguno de los derechos fundamentales del art. 18 CE, se deja en manos del juez instructor, para que sea quien autorice dicho acceso.

5.3. El problema de la jurisdicción y la ubicación de los datos electrónicos como objeto de investigación.

La regulación de alguna de las diligencias de investigación electrónica permite, actualmente, acceder y registrar los datos que están almacenados en dispositivos virtuales. Los datos albergados en "la nube" son susceptibles de ser analizados en la investigación de un delito. Estos servicios de alojamiento de información son considerados, a todos los efectos, como dispositivos por la LECrim, y por lo tanto y como tales, pueden ser registrados en busca de datos de interés para una investigación penal. Por ello, a partir de las siguientes líneas se va a analizar la cuestión referente a las implicaciones que el registro de estos datos ubicados en la nube puede tener en relación con la jurisdicción atribuida al juez instructor. Es decir, se trata de examinar con qué fundamento, de qué modo y mediante qué vías, el Juez puede ordenar que se acceda a estos servicios de almacenamiento de información en la nube, y se registren los datos que pudieran tener alojados.

Para responder a todas estas cuestiones conviene exponer qué instituciones y reglas sirven para atribuir la jurisdicción y competencia en general a los jueces y tribunales españoles. Posteriormente se expondrán las diferentes corrientes doctrinales que se postulan a favor y en contra de considerar que un Juez de Instrucción español tenga jurisdicción para acordar la diligencia de acceso y registro de los datos virtuales radicados en dispositivos situados en los territorios de otros Estados. En tercer lugar se expondrán algunas modalidades de auxilio con las que cuentan los tribunales para ejecutar estas actuaciones fuera de España, siendo algunas de ellas el resultado de las nuevas tecnologías[540].

5.3.1. La jurisdicción, el derecho a la tutela judicial efectiva y al juez predeterminado por la ley.

[540] Para conocer más sobre el particular, vid. GARCÍA PÉREZ, Rafael. «Los desafíos de la Unión Europea en la gobernanza global». *Cuadernos Europeos Deusto*. Núm. 45/2011. El número aborda íntegramente el concepto a través de diversos estudios centrados en materias muy dispares como la contribución de dicha gobernanza a resolver el cambio climático, cooperación y desarrollo, seguridad, etc.

El esquema legal español sobre las competencias judiciales parte del texto constitucional, que configura el derecho a la tutela judicial efectiva [541], del que derivan entre otros derechos, el del Juez predeterminado por la Ley.

El derecho a la tutela judicial efectiva se define por el Tribunal Constitucional como el «*derecho de todos a la jurisdicción, es decir, a promover la actividad jurisdiccional que desemboque en una decisión judicial sobre las pretensiones deducidas, en el bien entendido que esa decisión no tiene por qué ser favorable a las peticiones del actor, y que aunque normalmente recaiga sobre el fondo puede ocurrir que no entre en él por diversas razones. Entre ellas se encuentra que el órgano judicial instado no se considere competente. Ello supone que el art. 24.1 no puede interpretarse como un derecho incondicional a la prestación jurisdiccional, sino como un derecho a obtenerla siempre que se ejerza por las vías procesales legalmente establecidas, tal y como declaran los Autos de 30 de octubre de 1980 y 18 de febrero de 1981*»[542].

El derecho al juez predeterminado por la ley, por su parte, es *«el derecho fundamental que asiste a todos los sujetos del Derecho, a ser juzgados por un órgano jurisdiccional, creado mediante Ley Orgánica y perteneciente a la jurisdicción penal ordinaria, respetuoso con los principios constitucionales de igualdad, independencia e imparcialidad y sumisión a la Ley y constituido con arreglo a las normas comunes de competencia establecidas»*[543]. Es decir, el juez predeterminado por la ley es aquel órgano, con potestad jurisdiccional, que debe y que tiene que conocer de una determinada cuestión, y que está conformado previamente al conocimiento del concreto asunto, tanto formalmente como en la determinación de sus funciones y sus competencias[544]. Esto implica que está prohibido crear un órgano judicial con posterioridad al acontecimiento de un hecho penal, con la finalidad de obtener un determinado pronunciamiento, o la designación concreta de jueces

[541] Arts. 24 y 117 CE.
[542] STC 19/1981, de 8 de junio. Ponente: Don Ángel Latorre Segura. Fundamento jurídico segundo.
[543] Cfr. GIMENO SENDRA. Vicente. *Manual de Derecho Procesal Penal*. Colex- UNED. Madrid. 2014. Pág. 47.
[544] Sobre este derecho concreto cabe invocar el contenido de la STC 156/2007, de 2 de julio. Ponente: Don Javier Delgado Barrio. La sentencia describe en su fundamento tercero y cuarto el contenido de este derecho afirmando que «*es doctrina constitucional reiterada que dicho derecho exige, de un lado, la preexistencia de unas pautas generales de atribución competencial que permitan determinar, en cada supuesto, cuál es el Juzgado o Tribunal que ha de conocer del litigio (...), salvaguardando así la garantía de independencia e imparcialidad de los Jueces que conforma el interés directo preservado por aquel derecho y, de otra parte, que el órgano judicial llamado a conocer de un caso haya sido creado previamente por la norma jurídica, que ésta le haya dotado de jurisdicción y competencia con anterioridad al hecho que motiva su actuación y, finalmente, que por el régimen orgánico y procesal al que esté sometido no pueda calificarse como órgano especial o excepcional (...)*».

para determinados asuntos[545]. Todo lo anterior constituye una *«garantía para el justiciable de que podrá obtener un pronunciamiento libre de cualquier injerencia previa»*[546].

Estos derechos y garantías son aplicables a cualquier jurisdicción, pero son especialmente relevantes en el ejercicio del *ius puniendi*. El Estado, al valerse del derecho penal como derecho sustantivo y del derecho procesal penal como derecho instrumental[547], cuenta con enormes facultades, algunas tremendamente invasivas en la esfera de los derechos individuales. Como contrapartida se reconocen una serie de derechos al investigado, especialmente el derecho de defensa[548], así como la obligada observancia por el Estado del respeto a las garantías legales y procesales[549].

En consecuencia, las disposiciones sobre las funciones y competencias de los juzgados y tribunales, lejos de ser una formalidad, constituyen una verdadera garantía para el investigado, de modo que, si se producen actos procesales al margen de las disposiciones sobre competencia, el resultado obtenido será contrario al ordenamiento e incurrirían en un vicio de nulidad.

---

[545] La STC 31/1983 de 27 de abril. Ponente: Don Antonio Truyol Serra, estableció que "*una eventual irregularidad en la designación del Juez que ha de entender de un proceso puede constituir una infracción del derecho del justiciable al «Juez ordinario predeterminado por la Ley» del artículo 24.2 de la CE*".

[546] Cfr. DÍEZ-PICAZO JIMÉNEZ, I. «El derecho fundamental al juez predeterminado por la ley». *Revista Española de Derecho constitucional*. Año 11, nº 31. Enero – abril 1991. Página. 76.

[547] Se ha dicho que el derecho procesal penal es un *«instrumento esencial de la jurisdicción»,* así, Cfr. DE LA OLIVA SANTOS, Andrés. *Derecho Procesal Penal*. Centro de Estudios Ramón Areces. Madrid. 2000. Pág. 4. Con ello se da cauce a la expresión de muchos otros autores que destacan el papel del derecho procesal penal, que siempre queda un tanto a la zaga de la sustantividad del Derecho Penal en general. El mismo autor y dentro de la misma obra (Págs. 51-52) realiza una definición del derecho procesal penal, que considera al mismo desde dos ópticas, una digamos estrictamente doctrinal y la que aquí interesa, y que el autor considera como desde «*la perspectiva normativa»,* el «*Derecho procesal sería el conjunto de normas relativas a la estructura y funciones de los órganos jurisdiccionales penales (órganos del orden jurisdiccional penal), a los presupuestos y efectos de la tutela jurisdiccional concerniente al Derecho penal y a la forma y contenido de la actividad tendente a dispensar dicha tutela».*

[548] STC 181/1984, de 20 de junio. Ponente: Don Rafael de Mendizábal Allende. La resolución estableció incito al derecho de defensa «*no sólo la asistencia de Letrado libremente elegido o nombrado de oficio, en otro caso, sino también a defenderse personalmente [arts. 6.3 c) y 14.3 d) del Convenio y del Pacto más arriba reseñados] en la medida en que lo regulen las Leyes procesales de cada país configuradoras del derecho. Es el caso que la nuestra en el proceso penal (art. 739 de la Ley de Enjuiciamiento Criminal) ofrece al acusado* el "derecho a la última palabra" *(STS 16 de julio 1984), por sí mismo, no como una mera formalidad, sino —en palabras del Fiscal que la Sala asume— "por razones íntimamente conectadas con el derecho a la defensa que tiene todo acusado al que se brinda la oportunidad final para confesar los hechos, ratificar o rectificar sus propias declaraciones o las de sus coimputados o testigos, o incluso discrepar de su defensa o completarla de alguna manera". La raíz profunda de todo ello no es sino el principio de que nadie pueda ser condenado sin ser oído, audiencia personal que, aun cuando mínima, ha de separarse como garantía de la asistencia letrada, dándole todo el valor que por sí misma le corresponde. La viva voz del acusado es un elemento personalísimo y esencial para su defensa en juicio*» (F. 3)». Este derecho a ser oído se extiende incluso a la sentencia que vaya a ser dictada en apelación cuando de dicho proceso pueda derivarse una sentencia en la que se entre cuestiones de hecho y no sólo jurídicas. Sobre este concreto particular citaremos la STC 184/2009, de 7 de septiembre. Ponente: Doña Elisa Pérez Vera.

[549] El derecho a un proceso que respete todas las garantías se muestra en multitud de matices dentro de la instrucción penal, pues abarca con carácter general el respeto a los principios de inmediación y concentración, como puede verse en el contenido de la STC 167/2002 de 18 septiembre. Ponente: Don Vicente Conde Martín de Hijas. De ello puede desprenderse que los aspectos derivados del derecho a ser oído, de la necesidad de un efectivo control judicial (como por ejemplo el que debe llevarse a cabo cuando se intervienen comunicaciones, etc.), puede presentar relación con este derecho, además, y por supuesto con otros derechos de naturaleza constitucional también implicados. En esta misma sentencia se relaciona la falta de control de las intervenciones telefónicas ordenadas por el Juez, con el derecho al secreto de las comunicaciones, pero también con el derecho a un proceso con todas las garantías.

Las normas relativas a la jurisdicción y la competencia deben respetarse desde el inicio de la causa, y durante la práctica de los actos procesales que la misma exija. El juez instructor es competente para investigar los hechos con trascendencia penal que se le plantean, siempre que legalmente le vengan atribuidos, además no puede conocer de cualquier hecho penal de los que la ley le permite conocer, sino sólo de aquellos que sucedieron en un determinado lugar dentro de su partido judicial. Por lo tanto, aunque la actividad jurisdiccional y su competencia se extiende a la totalidad del territorio nacional, no puede ejercerse la misma libremente, ordenando realizar lo que se estima adecuado sin limitación alguna, sino que para ejecutar algunos de esos actos es necesario usar modalidades de actuación delegada[550]. En consecuencia, fuera del partido judicial, se debe acudir al auxilio de otros jueces del país, o la ayuda de jueces extranjeros en el ámbito de cooperación judicial internacional para la ejecución de actuaciones jurisdiccionales al amparo de convenios internacionales específicos.

Partiendo de esta premisa, puede concluirse que el juez instructor está habilitado para ordenar el registro de dispositivos de información que están dentro del territorio de su partido judicial e incluso fuera del mismo, pero dentro de territorio nacional, y que, sin embargo, habrá de recabar la cooperación de organismos judiciales extranjeros para llevar a cabo esta función cuando se realice fuera de nuestras fronteras.

Resulta, por tanto, que el juez de instrucción no puede, sin más, ordenar que se acceda y registren los datos dondequiera que estén, ignorando su paradero real, porque éste determina el modo de proceder adecuadamente, sin arriesgar la validez de la diligencia. Por eso es necesario conocer la ubicación de los datos informáticos a analizar.

En el caso concreto de las diligencias de investigación que se estudian en esta tesis, la ubicación de los datos electrónicos no tiene que ser un problema de falta de jurisdicción. El registro de un dispositivo de almacenamiento obtenido en un registro domiciliario, o incluso fuera de éste, no presenta problemas, porque los datos están en el interior del artefacto encontrado. Tampoco ha de haber problemas de competencia territorial derivado de un registro remoto, si el ordenador está ubicado dentro del territorio nacional, y los datos que se investigan están descargados en su memoria.

---

[550] Dispone el art. 4 de la LOPJ que *"La jurisdicción se extiende a todas las personas, a todas las materias y a todo el territorio español, en la forma establecida en la Constitución y en las leyes"*. Esto no supone olvidar la división territorial del Estado, que desde el punto de vista territorial- judicial y atendiendo al apartado V de la Exposición de Motivos de dicha Ley Orgánica se dispone que "*El Estado se organiza territorialmente, a efectos judiciales, en municipios, partidos, provincias y Comunidades Autónomas, sobre los que ejercen potestad jurisdiccional Juzgados de Paz, Juzgados de Primera Instancia e Instrucción, de lo Contencioso-Administrativo, de lo Social, de Vigilancia Penitenciaria y de Menores, Audiencias Provinciales y Tribunales Superiores de Justicia. Sobre todo el territorio nacional ejercen potestad jurisdiccional la Audiencia Nacional y el Tribunal Supremo"*.

Por el contrario, las dudas sobre el alcance de la jurisdicción del órgano instructor surgen en los registros de dispositivos virtuales, en los que la información que se analiza no está descargada en el ordenador o dispositivo, sino que éstos son el modo de acceso a tal información, normalmente alojada en el servidor de una empresa que presta el servicio y que puede estar materialmente ubicado en países muy distantes.

Esta clase de registros realizados sobre dispositivos virtuales exige por un lado que los agentes justifiquen de la necesidad de registrar este tipo de espacios, y asimismo deben informar de la posible ubicación de estos. Es deseable y exigible que esta información se encuentre en el oficio policial, y su necesaria aportación viene exigida por la obligación del juez de decidir sobre la práctica de la diligencia. Esta decisión debe adoptarse libre de toda incógnita sobre su jurisdicción y competencia territorial para acordar el registro del dispositivo virtual, y que, por tanto el Juez al conocer las circunstancias concurrentes en relación con la ubicación de los servidores que contengan los datos pueda adoptar las medidas de petición de auxilio especificas, evitando poner en riesgo la validez y eficacia futuras de la misma.

Por lo tanto, pese a que la ley no lo diga expresamente, el contenido del oficio, o bien un posterior complemento al mismo, debería proporcionar toda la información necesaria para adoptar una resolución judicial consciente de la posibilidad de que los datos estén alojados virtualmente fuera del territorio nacional. Para lo cual se deberán contener en el oficio policial cuanta información sea sobre: cuál es la empresa prestadora del servicio, dónde están ubicados sus servidores, si la misma cuenta con domicilio social en España o con un establecimiento abierto al público, y cualquiera similar.

Esta información se hace más necesaria en tanto que la legislación vigente, aunque permite el registro de datos alojados en la nube, lo hace sin clarificar correctamente alguno de los aspectos más controvertidos de esta acción, en especial el relativo a la ubicación de los datos. Puede decirse que se aprecia una colisión entre el contenido del Convenio de Budapest, suscrito por España, que sólo permite estos registros de datos virtuales cuando los datos están dentro del territorio del país que investiga, y la LECrim, que los permite sin haber introducido dicho matiz territorial, aunque sí hace referencia a otro tipo de requisitos relativos a la forma de acceso.

5.3.2. El problema de la evanescente ubicuidad de los datos alojados en la nube y la afectación de las competencias judiciales para acordar la diligencia de acceso a su contenido. Deficiencias en el contenido de la nueva regulación procesal.

5.3.2.1. Exposición del problema.

En apartados anteriores se ha esbozado el problema de jurisdicción y de competencia territorial que presenta la diligencia de registro de datos cuyo alojamiento está ubicado en la nube. Es momento ahora de desarrollar ese problema para, a continuación, analizar las pautas doctrinales que pretenden resolverlo.

El avance de los servicios de alojamiento de datos en la nube es innegable. Sus numerosas ventajas lo han convertido en un método cada vez más extendido para guardar información. En todo caso no son pocas las empresas que ofrecen estos servicios, que ubican los servidores que contienen estos datos en lugares que les resultan atractivos por la menor severidad legal en la protección de datos, por la existencia de estímulos fiscales y económicos o por su mayor implantación empresarial en ese territorio.

El ámbito procesal penal no puede sustraerse de esta evolución tecnológica, y ha comenzado a considerar, cada vez con mayor frecuencia, a los datos alojados en estos servicios, como a los que se guardan en otros dispositivos, como una innegable fuente de información, necesaria en la investigación criminal. Los datos que se contienen en estos dispositivos, una vez traducidos del lenguaje que presentan, al formato que corresponda, pueden arrojar información sobre un hecho delictivo. Estos datos, amparados en las posibilidades de acceso remoto que implica la nube, pueden ser transmitidos con extraordinaria facilidad de un lugar a otro. Esta volatilidad ha propiciado que diferentes países se coordinaran para concertar fórmulas de investigación criminal que permitieran localizar estos datos y examinarlos. Pero, pese a este esfuerzo, resulta paradójico que se haya dejado de lado esa facilidad para la transmisión de datos, y con ello ocultarlos de las autoridades, y se siga empleando el concepto civil de bienes muebles, apegado a la territorialidad de la ubicación, impidiendo una verdadera y rápida investigación.

El Convenio de Budapest, como instrumento internacional que ya ha sido examinado, es el instrumento de concertación internacional al que nos referimos. Este Convenio parte del concepto territorial de los datos, de manera que sólo permite que sean investigados penalmente los que están radicados en el territorio nacional.

La ley procesal española no ignora, ni extraña, el concepto de territorialidad. Las diligencias de registro de datos requieren tanto en su definición como en su desarrollo legal, como presupuesto para su aplicación, que nos encontremos ante artefactos radicados en territorio nacional.

Al mismo tiempo, la regulación española admite el registro de dispositivos que usan la nube, tal y como lo hace el Convenio de Budapest, pero no hay rastro alguno en el apartado 3, del art. 588

sexies c, ni el art. 588 septies a, 3, de regulación que se refiera expresamente a la ubicación territorial de los datos tal y como se recogía en el Convenio. Este es un aspecto positivo, que facilita la investigación trasnacional de datos, sobre todo teniendo presente que, a veces, esta ubicación territorial es imposible de determinar[551].

En suma, la LECrim admite el registro de datos en la nube, ignorando la ubicación real de estos datos y haciendo depender la práctica de la diligencia, de distintos presupuestos de acceso a la información, tal y como fue analizado en otros apartados.

Probablemente el apego territorial del Convenio de Budapest descansa en la importancia comercial de determinadas empresas del sector informático y lo que una liberalización completa de las posibilidades de acceso supondría en cuanto a la resolución internacional de conflictos[552]. Pero, aunque la finalidad de la legislación española es positiva, la redacción no clarifica si, con independencia del lugar en que se encuentren los datos, el Juez español cuenta con jurisdicción y competencia o no para registrar dichos dispositivos en la nube, en especial en el caso en que el acceso mediante el empleo del dispositivo del investigado no sea posible. Las posibilidades de interpretación de la redacción que se ha dado a estas diligencias es doble, o se entiende que está permitido hacer el registro de datos virtuales, sin mayores obstáculos más que el empleo del dispositivo o, por el contrario, hay que acudir a la cooperación judicial internacional para que sean las autoridades del lugar en el que están los datos, los recaben y los remitan al juez español.

El art. 588 bis, apartado b LECrim, y la interpretación conjunta de los apartados 1º, 3º, 4º y 6ª del mismo precepto, permite que se deba exigir de los investigadores la información suficiente en su solicitud sobre la posibilidad de que los datos estén en la nube. Por tanto, de modo complementario, el oficio deberá cumplimentar este aspecto concreto, esto es, habrá de contener indicación de la empresa con la que se tiene concertado el servicio de almacenamiento en la nube, así como si el repositorio virtual está radicado o no en España.

Además, y siguiendo el contenido del art. 588 sexies c. 3 LECrim, los investigadores deberían incluir también en su oficio de solicitud de la diligencia: la información acerca de la existencia o no

[551] Ver que este interrogante lo plantea Vid. MARTÍNEZ MARTÍNEZ. «El derecho y el Cloud computing» en MARTÍNEZ MARTÍNEZ (Editor). Op. Cit. Pág. 34, y en la misma obra Vid. ALAMILLO DOMINGO. «El control de localización de los datos e informaciones en el Cloud». Op. Cit. Pág. 64 y siguientes. En la obra se llega a considerar que, en algunos tipos de servicios, en concreto cuando lo que se ofrece es software, la localización se hace imposible.

[552] Sobre la normativa que en materia civil y mercantil sirve a los efectos de resolver conflictos internacionales sobre la materia referente a la protección de datos citamos a Vid. ORTEGA GIMÉNEZ, Alfonso. «Cloud Computing. Protección de datos y Derecho internacional privado (resolución de controversias y determinación de la Ley aplicable)» en MARTÍNEZ MARTÍNEZ RICARD (Editor), *Derecho y Cloud Computing.* Thomson Reuters- Aranzadi. Pamplona. 2012. Pág. 262 y siguientes, en las que se describe el mecanismo de resolución judicial de controversias suscitadas por una deficiente prestación de servicios relacionadas con la responsabilidad del agente prestador, aunque ceñidos a la jurisdicción civil.

de las claves de acceso a estos alojamientos virtuales, si existe otro medio de acceso legítimo, o cualquier otra información relevante sobre este particular. Toda esta información se convierte en un elemento imprescindible para que el juez pueda pronunciarse sobre la adopción, extensión, prórroga, modo de ejecución y cese del acceso y registro de datos, con garantía sobre la validez del resultado obtenido. La ausencia de esta información debería originar una respuesta judicial que consistiera en instar un complemento del oficio policial o directamente el rechazo de la diligencia solicitada, ante la falta de garantías en la efectividad de la medida interesada.

La redacción que habilita el registro de dispositivos en la nube no prevé ninguna medida alternativa si no se puede acceder a los datos tras encender el dispositivo. Sólo admite el acceso y registro si se conoce el usuario y la contraseña de acceso, o si el investigado la facilita, y claro está, los datos no están descargados en el ordenador. No hay ninguna previsión legal que marque la actuación a seguir si se ignora el paradero de los datos, por lo que no queda más opción procesal que, requerir a la empresa prestadora del servicio para solicitarle esos datos si cuenta con domicilio en España, y si no lo tuviera, hacerlo mediante los medios de cooperación judicial oportunos[553].

El mismo inconveniente concurre en la diligencia del art. 588 septies a, 3 LECrim, donde ni se alude a las inconveniencias derivadas de la ausencia de datos sobre el usuario y la contraseña, y donde tampoco nada se indica acerca de la cuestión referente a la ubicación de los datos.

Sin duda, hay muchos detalles de la práctica de estas diligencias que pueden depender del modo de acceso al ordenador, pero como se ha tenido ocasión de analizar previamente en este trabajo, la ley sólo detalla dos modos de acceso remoto, sin que se conozca, al menos desde un punto de vista jurídico, las implicaciones que los mismos pueden presentar.

Se han dados diversos pareceres doctrinales, que se verán más adelante, para resolver la interpretación que suscitan estos preceptos, pero se ha desperdiciado una oportunidad como la que representaba la regulación de este tipo de diligencias, para haber dado una mejor redacción al contenido de los artículos mencionados, bien dando plena libertad para acceder a los datos alojados en la nube con independencia del lugar en el que está la empresa suministradora del servicio, o bien dejando claramente sentado que será necesario acudir a una comisión rogatoria, o cualquier otro medio similar para llevarlo a cabo, incluso aunque esto pueda ralentizar, entorpecer o paralizar la investigación. En este concreto aspecto, se aprecia una vulnerabilidad en la protección de los derechos fundamentales del art. 18 CE, así como en un mejor desarrollo de la investigación penal, porque tanto una como otra cuestión dependen, en buena medida, de una correcta interpretación de

[553] En el apartado 3.3.3. *Mecanismos de cooperación judicial y otros métodos de auxilio*, de esta tesis se desarrollarán los diferentes métodos de cooperación judicial internacional, así como métodos y sistemas articulados para hacer más fluida dicha cooperación.

estas normas, dificultada por la oscuridad de la redacción actual. Esto, a la postre, impide al órgano encargado de velar por la tutela de los derechos fundamentales realizar sus funciones de manera adecuada[554].

Las posibilidades interpretativas, que se abren ante la vaguedad y falta de precisión de las normas ya citadas, han sido destacadas por la doctrina. Pero debe imponerse una interpretación lo suficientemente eficaz, que se conjugue con el contenido de pronunciamientos del Tribunal Constitucional [555] que han insistido en recordar que las medidas limitativas de derechos fundamentales deben recogerse expresamente en normas con rango legal suficiente que habiliten expresamente para llevar a cabo tal acción. Con ello podría darse la paradoja de que contando con previsiones normativas que habilitan para limitar el contenido de derechos fundamentales, y especialmente de los que se ven afectados en un registro de dispositivo de datos virtuales, no puedan llevarse a cabo estas medidas, bien por no quedar expresamente previsto un concreto modo de ejecutar la misma, al quedar fuera de la jurisdicción del Juez Instructor, bien porque la redacción de esta concreta forma de ejecutar la medida es difusa y no cuenta con una clara redacción que favorezca una interpretación acorde con el contenido de los derechos fundamentales que debe respetar.

5.3.2.2. Resolución de los problemas de jurisdicción en las diligencias de registro de datos en la nube. Posiciones doctrinales.

Una vez expuesto el problema consistente en cómo interpretar el art. 588 sexies c, apartado 3 de la LECrim, sobre el acceso y registro a los datos albergados en dispositivos virtuales puede apreciarse que hay dos aspectos en los que reside la controversia. Por un lado, está la propia mecánica o ejecución de la diligencia, la cual sólo puede realizarse mediante la concurrencia de las exigencias de acceso a los datos que contiene la propia ley, cuya interpretación y comprensión no resulta sencilla. El segundo aspecto es el que se deriva de la necesidad de tener que acceder a dichos datos

[554] El estado de la cuestión en lo observado de alguna sentencia parece decantarse de momento en favor de la idea de la territorialidad para proteger los datos excluyendo lo que no afecte a nacionales y a los datos que se alojen fuera del país. Puede verse sobre este aspecto la SAN dictada en el recurso 190/2016, de 21 de octubre de 2017, Ponente: Doña Felisa Atienda Rodríguez. La sentencia rechaza la petición de un ciudadano no nacional español para que se le aplique el derecho al olvido digital en nuestro país. Se da prioridad al derecho a la información y al orden internacional en la materia.

[555] Se trata de la STC 145/2014, de 22 de septiembre, y que ya se ha citado en otras notas de esta tesis. En síntesis, esta sentencia recuerda la necesidad de que cualquier medida de investigación procesal, que suponga una vulneración de los derechos fundamentales del investigado, debe estar expresamente prevista en la ley, en la medida en que dichos derechos fundamentales sólo pueden verse limitados aplicando medidas previstas en las leyes con rango suficiente.

usando otras vías distintas de las previstas en los arts. 588 sexies y septies, bien porque el acceso no sea posible en los términos descritos en la ley o por cualquier otra razón.

La deficiente redacción del texto de la Ley, cuando explica el modo de acceso a la información alojada en un dispositivo virtual, es el origen del problema. Los artículos referentes a la diligencia de registro de dispositivos de almacenamiento masivo de información comienzan admitiendo, con bastante amplitud, el acceso a múltiples dispositivos, tanto físicos o materiales como virtuales. Estos últimos dispositivos, los virtuales, entre los que se incluye la nube, están previstos en el contenido del art. 588 sexies a, LECrim, apartado primero, que considera susceptible de registro el «*repositorio telemático de datos»,* expresión que la doctrina estima que *«abarca todos aquellos instrumentos que incluyen entre sus funcionalidades la de servir de soporte para el almacenamiento masivo de datos»*[556]. Asimismo, el art. 588 sexies c, apartado 3, LECrim añade la posibilidad de registrar la información contenida en *"otro sistema informático o parte de él",* con lo que se redunda nuevamente en la idea de acceso y registro a esta clase de dispositivos, bien sea en su totalidad o bien en una parte de los mismos.

En lo que se refiere a la regulación de la diligencia de registro remoto de equipos informáticos, el art. 588 septies a, apartado primero LECrim también permite registrar, de modo virtual, un «*sistema informático, instrumentos de almacenamiento masivo o base de datos»*. Esta concreta diligencia, a diferencia del supuesto anterior, aunque admite el acceso virtual, no regula ni contiene precepto alguno sobre el modo de acceso. En suma, no puede albergarse duda alguna acerca de la posibilidad de examinar estos medios de almacenamiento de información virtuales, incluso mediante el empleo de un registro remoto, pues, la doctrina estima que estaremos en todo caso ante una modalidad de *«acceso a información accesible desde dispositivo incautado»*[557].

El modo de acceso a tales sistemas virtuales constituye uno de principales los problemas que ya se han advertido. Aunque la ley expone una serie de exigencias para proceder al acceso, sin embargo, la redacción que se le ha dado a estos requisitos de accesibilidad resulta bastante difusa.

En este concreto aspecto, el requisito que establece la ley para poder hacer el registro es la de exigir, con carácter previo, que *"los datos sean lícitamente accesibles por medio del sistema inicial o estén disponibles para éste*". En especial, la expresión *«estén disponibles para este»* parece ser el *quid* de la cuestión porque permite muchas interpretaciones. El tenor del precepto establece que para que

[556] De hecho, algunos autores precisan que también son dispositivos de almacenamiento de información, los aparatos interconectados entre sí, apoyándose en el Convenio de Budapest sobre ciberdelincuencia. Así, Cfr. LÓPEZ-BARAJAS PEREA, Inmaculada. «Nuevas tecnologías aplicadas a la investigación penal: el registro de equipos informáticos». *Revista de Internet derecho y política*. IDP N.º 24 (Febrero, 2017) I. Pág. 71

[557] Cfr. DELGADO MARTÍN, Joaquin. «Investigación del entorno virtual: el registro de dispositivos digitales tras la reforma por LO 13/2015». *Diario La Ley*, Nº 8693, 2 de Febrero de 2016. LA LEY 229/2016. Págs. 3 y se desarrolla a lo largo de la pág. 10.

pueda realizarse un registro a un dispositivo virtual, es necesario un acceso simple al mismo, sin operaciones adicionales que lo permitan, o bien que se conozca previamente a realizarlo cuál es el modo de acceso habitual a dicha información, por ejemplo, teniendo la clave de usuario y la contraseña de acceso. Lo más probable es que la expresión signifique que no sea necesario realizar operación alguna en el instrumento intervenido para acceder a los datos, pues sólo de este modo se da verdadera disponibilidad.

Por lo tanto, si el acceso se produce tan solo encendiendo el dispositivo o abriendo una aplicación, y no hay que hacer nada más para consultar la información, se entiende que los datos a los que se acceda de este modo es que están disponibles.

En resumen, lo que parece exigir la ley es que no sea necesario introducir siquiera un usuario o una contraseña. La doctrina defiende esta interpretación cuando estima como requisitos de acceso: *«a. Que el ordenador o dispositivo se encuentre abierto y sea posible acceder al contenido almacenado en la nube sin necesidad de utilizar las claves y contraseñas del usuario. b. Que se conozcan las claves y contraseñas que permiten el acceso al dispositivo y en su caso a la nube porque se han obtenido por distintas vías: las ha proporcionado voluntariamente el propio imputado, se han obtenido en el curso de la investigación previa, se han conocido mediante el empleo de técnicas de ingeniería social, o se extraen del análisis técnico o forense del ordenador o dispositivo incautado»*[558].

No obstante, estas situaciones parecen tan improbables en la práctica que no serán las más habituales. Las claves de acceso a los dispositivos son cada vez más frecuentes, y van dejando atrás los habituales medios de descripción de usuario y contraseña, para dar paso a la realización de un dibujo pautado, el uso de reconocimiento por huella dactilar, o por vía facial, incluso por el ritmo cardiaco. Esta personalización del acceso a un dispositivo hace que la disponibilidad que exige nuestra LECrim concurrirá en pocos casos. Por lo tanto, se impone la necesidad de reinterpretar el concepto de accesibilidad de los datos, de manera que no quede comprometida la legalidad del registro pese a que implique realizar operaciones en el ordenador.

Por su parte, en lo que se refiere a la diligencia de registro remoto, pese a que también se admite el registro virtual, no se dice nada de cómo realizarlo, ni tampoco se dan criterios que sirvan para ejecutar la medida de esta manera, como sí sucede con la diligencia del art. 588 sexies LECrim.

---

[558] Cfr. MARTÍN MARTÍN DE LA ESCALERA, A, M. «El registro de almacenamiento masivo de la información. Ponencias de Formación organizadas por la Fiscalía General del Estado». Jornadas de 27 de abril de 2016 tituladas "La interceptación de las Comunicaciones telefónicas y telemáticas". Texto contenido en el enlace web: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20Martín%20Martín%20de%20la%20Escalera,%20Ana%20Mª.pdf?idFile=bf66c357-e4d4-4701-8a4d-83d6c103ebe5. Pág. 21.

En realidad, este silencio puede interpretarse en el sentido de que, dado que existe autorización para acceder remotamente a todo o parte del equipo y la finalidad perseguida es obtener los datos de interés, no parece importar al legislador que tal información esté dentro del equipo, debidamente descargada, o por el contrario se aproveche la intervención del mismo para acceder a los datos que el usuario consulta o consigue accediendo voluntariamente a dicho dispositivo virtual. En todo caso el registro en esta segunda clase de diligencia no puede realizarse amparándose en razones de urgencia, ni por la policía, ni por el Ministerio Fiscal, con lo que será el auto el que habrá definido el sentido del registro, de manera que, si se requiere el examen de alguna otra ubicación donde la misma información esté alojada (carpetas virtuales o similares), se necesitará una nueva solicitud y un nuevo auto.

El otro problema que se mencionaba al inicio de este apartado, y que no es sino consecuencia de lo anterior, es qué hacer en el caso de que existan dudas acerca del modo de acceso a la información virtual. Más concretamente, lo que cabe cuestionarse es si la decisión que adopte un Juez en orden a registrar la información alojada en un dispositivo virtual, en caso de duda sobre el método de acceso, exige saber dónde están dichos datos para poder articular medios de acceso a la misma, mediante instrumentos de auxilio judicial o de cooperación judicial internacional.

Esta última consideración se expone en la medida en que la jurisdicción del Juez instructor puede estar en entredicho, pues si el mismo decide ordenar un registro de un dispositivo para el que no cuenta con accesibilidad inmediata, este proceder podría tener como consecuencia la nulidad de lo actuado, bien sea por ser contraria la decisión al tenor de la ley, bien por haber accedido directamente ignorando el lugar en que se encuentren los datos, sin haber acudido a las vías de auxilio o cooperación judicial internacional. Es más, cabe admitir que incluso en el caso en que se permitiera el acceso a la nube, la cuestión de la ubicación de los datos relacionada con la jurisdicción o no del Juez no queda resuelta. El Juez español no puede unilateralmente acceder a cualquier evidencia sin tener en cuenta dónde se encuentre. Cuando las evidencias están fuera del territorio nacional necesita de la cooperación y del auxilio de otros jueces ubicados en los territorios en que esas evidencias se encuentren.

En suma, de lo que se trata es de no renunciar al registro del dispositivo, sino que su realización exige acudir a las vías de ayuda internacional, para que sea el juez del lugar en el que están los datos el que los recabe y entregue.

Las posiciones doctrinales a estos interrogantes son muy variadas, abarcando todas las opciones posibles, lo que subraya la existencia de una importante controversia sobre el particular. Algunas de estas opiniones, tratan de resolver el asunto mediante una interpretación extensiva de las normas

procesales que permiten el registro, admitiéndolo con independencia de la ubicación final de los datos[559].

Otros pareceres consideran que sólo cabe realizar el registro prescindiendo de la ubicación geográfica de los datos en casos muy contados, usando para eso el ordenador o el dispositivo encontrado y el acceso que éste permite sin mayores manipulaciones[560], y otras estiman que se debe acudir a mecanismos de cooperación judicial distintos y alternativos al propio tenor literal de la ley[561]. En todo caso muchas de estas posiciones se entremezclan en ocasiones, y comparten, en ocasiones, algunos puntos comunes.

En general, todas estas posiciones, pueden dividirse, con muchos matices, en dos grupos fundamentales: las que estiman que el juez español es competente para ordenar el acceso y registro de los datos alojados en la nube, incluso cuando se encuentren fuera del territorio nacional, y otras que estiman que ello no es posible. Entre estas dos posiciones extremas, existe un tercer grupo de opiniones, que defienden que nuestra norma procesal no habilita los registros en la nube, y consideran que para llevarlos a cabo hay que acudir a normas de cooperación judicial internacional. Pasaremos a describir los argumentos que se dan dentro de cada postura para sustentarla.

I) Los que defienden que el juez tiene jurisdicción en todo caso para ordenar el acceso y registro de los datos alojados en la nube, con independencia del lugar en que estén esos datos, argumentan su posición utilizando los siguientes argumentos:

a) La posibilidad de perder los datos. Dado que el depósito de datos en la nube los hace proclives a una fácil modificación e incluso desaparición (volatilidad), debe estimarse, como contrapartida a esa volatilidad de la información, que el juez español tiene jurisdicción para ordenar directamente el acceso y el registro de los datos que estén almacenados en la nube, donde quiera que se encuentren los servidores que la alojen, y que incluso el registro pueda

[559] Estas posiciones se desprenden de los trabajos de RODRÍGUEZ LAINZ, José Luis, CUADRADO SALINAS, Carmen y de CONDE-PUMPIDO TOURÓN, Cándido, que se citarán y analizarán dentro de este mismo apartado, y donde se expondrán los argumentos y razonamientos más relevantes que se siguen para justificar esta postura

[560] La Fiscalía General del Estado es partidaria, con matices, de esta postura, así como también sostienen argumentos favorables a este posicionamiento VALVERDE MEGÍAS, Roberto y LÓPEZ BARAJAS PEREA, Inmaculada. Seguidamente se expodrán y citarán sus trabajos, así como el análisis de cada uno de los argumentos empleados para sostenerlos.

[561] Este parecer es el que parecen sostener algunos miembros de la judicatura, por ejemplo DELGADO MARTÍN, Joaquín, y también por parte de MARTÍN MARTÍN DE LA ESCALERA, A, M, cuyos trabajos serán citados seguidamente así como también los argumentos empleados para justificar esta posición.

hacerse por parte de los agentes investigadores, por fundadas razones de urgencia[562]. El fundamento técnico de esta postura es innegable. Las operaciones de borrado de datos son muy simples de realizar empleando los servicios en la nube, y además es altamente probable que puedan producirse con la clara intención de eliminar todo rastro delictivo. En este sentido, no debe perderse de vista que la principal ventaja de los servicios *en la nube* es que están disponibles desde cualquier lugar y dispositivo, y basta sólo con tener acceso a internet, lo que hace que una operación de borrado de datos pueda hacerse desde cualquier país, desde cualquier ubicación y en cualquier momento. Además, no tiene que hacerlo ni siquiera el investigado, sino que cualquiera con quien se comparta la información, o quien sospeche que está siendo investigado podrá deshacerse de ella o trasladarla a otro alojamiento virtual. Precisamente todo esto apoya y justifica la necesidad de una rápida actuación que se vería frenada de tener que acudir a vías de cooperación judicial internacional lentas y farragosas. Por lo tanto, estas razones de volatilidad de la información justificaría que los agentes investigadores accedieran a ella, y por consiguiente habilita al juez para ordenarlo a pesar de encontrarse el servidor radicado en el extranjero.

b) La exigencia de nuevos tipos de investigación y de nuevas prácticas de investigación. Esta opinión se funda en que el registro digital es un modo de acceso a datos diferente al actual registro de papeles o al de un domicilio. Es una tipología de registro diferente a aquéllas porque se accede a «*impulsos electrónicos (objetos intangibles)*»[563]. El argumento que sustenta esta posición considera que se encuentra ante un objeto de investigación distinto, y por eso no puede justificarse el registro virtual de datos mediante la aplicación de la regulación legal y la doctrina jurisprudencial elaborada sobre el registro de objetos

[562] Cfr. RODRIGUEZ LAINZ, José Luis. «Registro policial de dispositivos de almacenamiento masivo de datos por razones de urgencia. Comentario a la Sentencia del TEDH del caso Trabajo Rueda vs. España». *Revista Juridica editorial Sepin*. SP/DOCT/22992. Pág. 5. El autor justifica de esta manera el acceso de emergencia que pueden realizar las Fuerzas y Cuerpos de Seguridad del Estado. Lo importante en todo caso es que, si con independencia de su ubicación, pueden los investigadores acceder a la información más razón cabe para seguir el mismo razonamiento hacia el Juez. No obstante, sería interesante analizar un caso concreto como este en el que parece que los investigadores alcanzan mucha más competencia que el propio Juez. Dice textualmente: *« La generalización de la conservación e interactuación de datos procedentes de un dispositivo de almacenamiento de datos con bases de datos externas –datacenters– o los alojamientos en la llamada nube –cloud computing– ha supuesto que buena parte de la información asociada a un concreto dispositivo informático conectado a la red haya de buscarse precisamente fuera de la memoria interna del dispositivo; con el riesgo que ello comporta de destrucción o alteración de forma remota, aprovechando claves de usuario, desde cualquier otro dispositivo y mientras se espera a la decisión de la autoridad judicial. Un registro extendido a tales fuentes externas, en los términos a los que se refiere el actual art. 588 sexies c).3 LECrim., se muestra claramente vulnerable a la posibilidad de destrucción o manipulación; frente a los que, dándose las circunstancias, no cabrá otra opción a la unidad policial actuante, que, bien proceder a la anticipación en la medida de extensión, con posterior ratificación judicial, o emitir, de ser viable, una orden de congelación/conservación de datos al amparo de lo establecido en el art. 588 octies.*».

[563] Cfr. CUADRADO SALINAS, Carmen. «Registro informático y prueba digital. Estudio y análisis comparado de la ciberinvestigación criminal en Europa (1)». *La Ley Penal,* Nº 107, Marzo-Abril 2014. LA LEY 1257/2014. Pág. 3 y 4. La autora defiende nuevos métodos de acceso y de registro para nuevos modos de guardar la información. Pone como ejemplo el caso de Inglaterra en el que este tipo de acceso y de registro se guía por otras reglas distintas a las expuestas.

corpóreos y palpables, que implican necesariamente estar ante la cosa o el lugar que es objeto de la diligencia. En cambio, un registro virtual no exige estar presente en el lugar en que está el objeto a registrar, y por consiguiente el acceso, registro, análisis e interpretación de los datos digitales deben contar con una nueva justificación y fundamento, distinto a las vías tradicionales.

c) La ubicación de los datos es irrelevante en los registros virtuales. Esta idea también sirve a quiénes consideran que la ley otorga jurisdicción al juez para ordenar el registro de los datos ubicados en la nube, prescindiendo del lugar en que radiquen los servidores en que se aloje la nube. El fundamento de esta posición parte de la forma en que se accede y registran estos datos. Estos autores consideran que como la vía de acceso a la información es digital, puede prescindirse de la localización de los datos, porque el modo que se emplea para poder acceder y registrar los mismos es también digital[564], con ello se prescinde del criterio de ubicación y se fundamenta la jurisdicción en el modo de realizar el registro.

d) La competencia territorial viene determinada por el lugar en el que se encuentra el dispositivo desde el que se accede a la nube. Esta postura funda la jurisdicción en un concepto territorial, aunque con el matiz de que el concepto de territorio no debe entenderse como el lugar en el que están los servidores que alojan los datos, sino que la jurisdicción viene determinada por el lugar en el que se haya incautado el dispositivo que permite el acceso a dichos datos. Por consiguiente, si el dispositivo que se usa para acceder a los datos se ha ocupado o incautado en España, es el juez español el que puede ordenar su registro. Quiénes apoyan esta opinión mantienen que «*la tutela de los derechos fundamentales no puede quedar a la decisión del gestor de un servicio informático (ejemplo de Google) sobre el lugar que elija para ubicar los medios técnicos desde los que lo presta, máxime cuando opera y la infracción penal produce efectos dañinos en el país que trata de perseguir el delito, cuando los dispositivos/terminales se hayan ocupado y el delito haya producido efectos, por ejemplo, en España»* [565].

[564] Cfr. CONDE-PUMPIDO TOURÓN, Cándido. *La reforma procesal. Registro de sistemas informáticos, ampliación del registro a otros sistemas. El registro remoto de dispositivos informáticos (arts. 588 sexies y 588 septies LECRIM)*. Ponencia presentada en las Jornadas de formación organizadas por la Fiscalía General del Estado con fecha 10 de marzo de 2016 en materia de criminalidad informática. Pág. 17, se dice textualmente: *«o una vez se habilita otra vía de acceso, debería ser admisible que las autoridades judiciales españolas conocieran los contenidos archivados en la nube sin necesidad de acudir a los mecanismos de cooperación judicial internacional.»*

[565] Cfr. VELASCO NUÑEZ, Eloy. "Investigación procesal penal en redes, terminales, dispositivos informáticos, imágenes, GPS, balizas: la prueba tecnológica". *Diario la Ley*, nº 8183, sección doctrina, 4 de noviembre de 2013. La Ley 8334/2013. Pág. 11.

La nota común a todas estas posiciones doctrinales, que defienden la competencia del juez para ordenar el registro de datos en la nube cualquiera que sea la ubicación de los datos, es su carácter innovador y claramente rompedor. La finalidad que se persigue no es otra que evitar un retardo innecesario en la investigación, derivada de los trámites para solicitar la cooperación judicial internacional, o de la negativa de las empresas tecnológicas a la entrega de los datos solicitados, bajo la coartada de no estar en posesión de la información requerida por estar en una filial extranjera a la que el derecho español no alcanza.

Sin embargo, a estas posiciones doctrinales se les puede objetar que no cuentan con amparo normativo, porque son las leyes las que determinan los límites de la jurisdicción española para realizar ésta y otras diligencias, y aunque realmente algunas de sus consideraciones pueden resultar bastante ajustadas a las concepciones actuales del empleo de medios tecnológicos, no cuentan con el suficiente respaldo jurisprudencial.

Junto con este primer grupo que defiende la competencia del Juez español para registrar los datos en la nube, hay otro grupo de autores, que, defendiendo esta posición, se basan en criterios más moderados. Entre estas opiniones, los argumentos que se emplean son los siguientes:

a) El juez instructor es competente para registrar los datos alojados en la nube porque su jurisdicción se lo permite. Estiman que, si el delito se investiga en España, hay jurisdicción para practicar todas las diligencias que sean necesarias para culminar dicha instrucción [566].

b) El juez instructor puede ordenar el registro de la nube, amparado en razones técnicas. Para este segundo grupo de autores, el juez tiene jurisdicción para registrar los datos de la nube independientemente de la ubicación del servidor que los aloja. En concreto se basan en el hecho de que como los datos pasan directamente del servicio en la nube hasta el ordenador del investigado, y dicho dispositivo se encuentra físicamente en España, el juez es competente para acceder y registrar su contenido [567]. Esta posición ha sido finalmente acogida por la Fiscalía General del Estado en el informe presentado al anteproyecto de Ley

[566] Vid. DE LA ROSA CORTINA, José Miguel. Acceso a ordenadores, dispositivos electrónicos y sistemas de almacenamiento masivo de memoria. Acceso remoto. Acceso a la nube. Ponencia del Curso sobre Intervención de las Comunicaciones Telemáticas, Centro de Estudios Jurídicos del Ministerio de Justicia. Madrid. 22 de mayo 2014. Págs. 33 y 34. El enlace puede consultarse en: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20escrita%20Sr%20de%20la%20Rosa%20Cortina%20(2).pdf?idFile=3d0616d9-3c76-4d41-9e37-de5c8ffcab78

[567] Vid. VALVERDE MEGÍAS, Roberto. *Intervención de comunicaciones telemáticas y registro remoto*. Ponencia realizada en los cursos de formación continuada realizados en fecha 27 de abril de 2016 bajo la denominación de *La interceptación de las comunicaciones telefónicas y telemáticas*. Pág. 29 y siguientes. Puede encontrarse el texto íntegro en el enlace de la página de Ministerio Fiscal: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20Valverde%20Meg%C3%ADas,%20Roberto.pdf?idFile=c740b0e1-8842-4ef7-8983-23c4a0732291

Orgánica de reforma de la LECrim[568], y sigue siendo el criterio que viene sosteniendo en la Circular 5/2019, de 6 de marzo. En esta última Circular, si bien se aconseja acudir a los mecanismos de cooperación judicial internacional en los casos más dudosos, entiende que el juez español cuenta con jurisdicción para registrar la información alojada en los repositorios de datos, porque se trata de datos que conforman el sistema que se registra, siendo lo determinante a efectos de determinar la competencia, el lugar en que está el dispositivo que alberga el sistema, y no el lugar en que están los datos . El supuesto de un registro de datos alojados en la nube realizado mediante la práctica de la diligencia de registro remoto, la Fiscalía General del Estado se muestra mucho más exigente con la necesidad de que exista una clara vinculación territorial con España.

c) Prescindir completamente de cualquier criterio relacionado con la territorialidad o la ubicación de los datos. En esta misma línea hay autores que, prescindiendo de la idea de ubicación de los datos, mantienen que *«ante la imposibilidad absoluta o práctica imposibilidad de localización, debería no tener que aplicarse un igualmente imposible principio de territorialidad»*[569] e instan a sustituirlo por criterios como el de la «*ubicación del sistema inicial sometido a registro, bien la jurisdicción del prestador del servicio de alojamiento»*[570]. Este conjunto de opiniones no cuenta, hasta el momento, con el respaldo jurisprudencial que sería deseable, y además parecen contrarias a la norma española vigente,

[568] El Informe al Anteproyecto de Ley Orgánica de reforma de la LEcrim efectuado por el Consejo Fiscal, (puede consultarse el enlace en la página web: http://pdfs.wke.es/2/2/7/8/pd0000102278.pdf), dice específicamente en su página 115, apartado 5.16.3 que "*El apartado cuarto del art. 588 bis g se refiere a los supuestos en los que la información se encuentra alojada en otros sistemas o en servidores disponibles en el cloud computing dadas las facilidades de almacenamiento que ofrece esa tecnología y la posibilidad del cliente o usuario de obtener la información en cualquier momento a través de su propio dispositivo informático»*. Sin embargo, el finalmente aprobado art. 588 bis apartado g de la LECrim no hace alusión a ninguno de los aspectos que menciona este informe de la Fiscalía. De hecho, con la lectura de dicho anteproyecto se constata que efectivamente contenía un texto exactamente igual al que en la actualidad se contiene en el art. 588 sexies c, apartado 3, que por supuesto está sólo referido a la diligencia de acceso a dispositivos de almacenamiento masivo de información, y que en el anteproyecto estaba pensado con carácter general también como disposición aplicable a cualquier medida de intervención en los derechos del art. 18 CE, pero que finalmente no fue incluida. El mismo informe de la FGE hace alusión (ver pág. 124) a la necesidad que puede darse de tener que consultar datos necesarios para la investigación obrantes en servicios remotos. Ante esta circunstancia la propia fiscalía alude a que «*debiera preverse la posibilidad de que el acceso a información contenida en sistemas de cloud computing se autorice por las autoridades judiciales españolas»,* pero consciente de los problemas de competencia territorial que ello puede suponer alude acto seguid que ello será posible «*siempre que nuestros tribunales tengan jurisdicción para conocer de la causa que se está investigando».* Sin embargo, tan ortodoxa declaración queda más tarde un tanto deslucida al seguir un criterio conforme al cual difumina tal exigencia por el mero hecho de que la información pudiera resultar visible desde España, como elemento que por sí solo justificaría el acceso a la información declinando la exigencia de cualquier ayuda al exterior. Más tarde en la pág. 123 del Informe se dice claramente que la cuestión no se resuelve en el anteproyecto, pero que debiera hacerse. Aporta el criterio de la jurisdicción para conocer del delito como justificante de la adopción de medidas de intervención fuera del territorio nacional.

[569] Cfr. RODRÍGUEZ LAINZ, José Luis. «Registro de dispositivos de almacenamiento masivo de información». Comunicación presentada en el curso Ciberdelincuencia. Problemática penal de las redes sociales, celebrado en Valencia los días 9 y 10 de marzo de 2017. Pág. 23 (texto original no publicado).

[570] Cfr. RODRÍGUEZ LAINZ, José Luís. «Registro de dispositivos …». Op. Cit. Pág.23.

que se basa en el criterio de territorialidad de los datos, que está muy presente también en el contenido del Convenio de Budapest sobre ciberdelincuencia, que ya se analizó en otros apartados y que constituye derecho interno. En todo caso serían criterios que podrían ser asumidos jurisprudencialmente como fórmula de interpretar el acceso lícito.

d) Prescindir de la territorialidad y sustituirla por una habilitación otorgada por consentimiento del investigado. Los defensores de esta interpretación admiten la posibilidad de registro de la nube sólo en los casos en los que se cuente con la autorización del investigado, y cuando se trate de información públicamente disponible. En todo caso se muestran reticentes con que se pueda acceder a la nube cuando los datos están fuera del territorio nacional [571]. Esta opinión es la que más se acerca al contenido del art. 588 sexies c, párrafo 3 LECrim, que admite el registro de datos alojados en repositorios cuando el acceso es lícito, licitud que evidentemente concurre cuando se cuenta con el consentimiento del afectado. El concepto de información públicamente disponible, que para los defensores de esta postura es el segundo criterio que admite el registro de datos con independencia del territorio en el que estén, presenta el problema de ser un concepto indeterminado. Además, parece una categoría un tanto innecesaria, porque no se encuentra problema alguno en tomar la información que es pública, lo que priva de utilidad el registro, con lo que los problemas jurídicos derivados del mismo se desvanecen.

e) Prescindir del criterio de territorialidad por razones de urgencia. Los seguidores de esta posición mantienen la admisibilidad del registro de datos alojados en la nube, sin perjuicio de admitir la problemática de la jurisdicción, cuando se realice por motivos excepcionales que habrán de ser deslindados y configurados por la jurisprudencia[572]. A este criterio le es objetable la ausencia de definición de las razones de urgencia que podrían motivar dicho registro. Además, teniendo presente que la legislación procesal contempla la posibilidad de que estas razones las aprecien los investigadores o el Ministerio Fiscal, se hace necesario que se definan algo más dichas circunstancias, como ya se dijo en otros apartados de este estudio. Por ello esta posición tampoco resuelve los problemas derivados de la falta de garantías en la observancia, graduación y determinación de lo que se entienda por razones de urgencia.

---

[571] Cfr. LÓPEZ-BARAJAS PEREA, Inmaculada. «Nuevas tecnologías aplicadas a la investigación penal: el registro de equipos informáticos». Op. cit. Pág. 71. Dice autora textualmente: *«También se permite el acceso transfronterizo a los datos almacenados, pero solo cuando se trate de datos de libre acceso al público o con el consentimiento lícito y voluntario de la persona legalmente autorizada para divulgarlos a través de ese sistema informático.Fuera de estos supuestos, la autoridad investigadora debe remitir la correspondiente solicitud de asistencia judicial internacional».*

[572] Vid. BACHMAIER WINTER, Lorena. «Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015». *Boletin del Ministerio de Justicia*. nº 2195. enero 2017. www.mjusticia.es/bmj. Pág. 27.

II) En una línea intermedia entre los autores que defienden que el juez instructor cuenta con jurisdicción para ordenar el registro de datos alojados en la nube, incluso aunque estén fuera de territorio nacional, y los que opinan lo contrario, existe un grupo de autores que ofrecen una opinión intermedia entre estas dos, apartándose de la territorialidad como problema, y considerando otros aspectos distintos para denegar la competencia al juez instructor a la hora de registrar los datos en la nube.

Entre estas posiciones destacan los siguientes argumentos en favor de la postura:

a) Los que consideran que la polémica no debe estar tanto en la territorialidad del repositorio virtual en el que esté alojada la información, sino en que hay que discriminar qué tipo de datos son los que hay que registrar. Estiman que la regulación actual no es suficiente para resolver la protección de algunos de estos datos alojados en la nube. Los que defienden esta posición parten del texto constitucional, y de su regulación sobre la protección del honor y la intimidad, que no permiten mas que el consentimiento del interesado para su limitación. Excluida cualquier otra clase de tutela legal para la protección de este tipo de datos, ya que el texto constitucional no alude a la necesidad de que se pueda sustituir el consentimiento del afectado por una resolución judicial, sólo quedaría la tutela que brinda a estos derechos la Ley Orgánica de protección del derecho al honor y a la intimidad familiar [573]. A estos razonamientos le serían esgrimibles los condicionantes derivados de la nueva doctrina sobre el entorno virtual, según la cual no se protege una sola dimensión de los datos, sino que se protege una conjunción o agrupación de todos ellos cuando se trata de realizar alguna diligencia de investigación electrónica, y tal protección se realiza y se colma mediante la autorización judicial.

b) Las que consideran que la ausencia de localización de los datos no puede limitar o perturbar la investigación, sino que hay que acudir a aspectos basados en las empresas prestadoras de los servicios de alojamiento de datos en la nube. Bajo esta premisa se considera que si el dispositivo desde el que se accede a la información, y el prestador de servicios que posibilita dicho acceso a la red, están en territorio nacional, existe una presunción de la legalidad del acceso[574]. Esta misma parte de la doctrina alude a la posibilidad de considerar a empresas no

[573] Vid. ZOCO ZABALA, Cristina. *Nuevas tecnologías y control de las comunicaciones*. Thomson Reuters - Aranzadi. Navarra. 2015. Pág. 74 a 78 y 89.

[574] Cfr. RODRÍGUEZ LAINZ, José Luis. «Tres cuestiones polémicas sobre el registro de dispositivos electrónicos de almacenamiento masivo de información», apartado dedicado a: ¿Se podría legítimamente acceder a información contenida en la nube a través de un registro de dispositivo electrónico de comunicaciones?. Op. Cit. Pág. 4. El autor dice textualmente que : *«Si partimos de la base de que tales alojamientos prácticamente no tienen una ubicación física definida, al ser esta de imposible o muy difícil determinación, no contaríamos con más referentes territoriales que el propio del dispositivo de comunicaciones sometido a un registro físico, y, por tanto, ubicado en el espacio*

radicadas en el territorio de la Unión como agentes obligados al suministro de información, aunque sus propios defensores reconocen que es una cuestión polémica e insegura [575].

Todas estas opiniones pueden servir para fundar, con mayor o menor éxito la licitud del acceso que requiere el tenor del art. 588 sexies c 3 LECrim, pero, en cambio no justifican tanto el requisito de disponibilidad de la información de la que habla dicho precepto, que queda inexplicado, desarrollado e interpretado por la doctrina. Ante esta indefinición, y dada la ausencia de jurisprudencia o acuerdo de pleno no jurisdiccional de la Sala Segunda que matice el alcance de la jurisdicción necesaria para acceder a los datos situados en la nube, la doctrina mantiene que *«si la información se encuentra alojada en servidores ubicados fuera de territorio nacional no quedará más solución que la de acudir a los medios de cooperación internacional, a salvo aquellos casos, excepcionales»*[576].

Las resoluciones dictadas hasta el momento por distintos tribunales, y a falta de lo que pueda decir el Tribunal Supremo, admiten el registro virtual sin detenerse en la ubicación de los datos, lo que permite apreciar bastante flexibilidad en la aplicación de los requisitos exigidos en el art. 588 sexies c 3 LECrim, a la hora de acordar la práctica de la diligencia de registro de datos en espacios virtuales[577].

En el seno de la judicatura tampoco existe un parecer único y hay división de opiniones entre los que justifican y admiten el acceso y registro de datos en la nube de modo directo y sin limitaciones territoriales; mientras que otros defienden el registro de datos, pero mediante el empleo de medidas de cooperación judicial internacional[578].

---

jurisdiccional de una autoridad nacional; así como el del ámbito territorial del prestador del servicio a través del cual el sujeto investigado, o el dispositivo en cuestión, ha alojado la información objeto de indagación en la nube. El que una determinada información esté alojada en la nube no puede convertirse en una patente de corso de apatridia que la hiciera inmune a cualquier introspección hasta que se descubriera cuál es su ubicación física, única o plural. No nos cabe otra opción que la de excepcionar de tal criterio de territorialidad los alojamientos en la nube; al menos ante aquellas contingencias en que resultara imposible o especialmente gravoso indagar su localización física».

[575] Cfr. RODRIGUEZ LAINZ, José Luis. «¿Podría un juez español obligar a Apple a facilitar una puerta trasera para poder analizar información almacenada en un iPhone 6?»". *Diario La Ley*, Nº 8729, 28 de Marzo de 2016. Pág. 7.

[576] Cfr. MARTÍN MARTÍN DE LA ESCALERA, A, M. Op. Cit. Pág. 22.

[577] Autos de la Audiencia Provincial de Barcelona, Sección 5ª, de fechas 1 y 16 de marzo de 2017, con números 214/2017 y 251/2017. Ponentes: Doña Elena Guindulaín Oliveros y Don José María Assalit Vives. En ambos autos se ordena la descarga de la información contenida en la nube en el ordenador del investigado y desde ahí se ejecute su volcado, sin que se plantee por parte del órgano instructor, ni por Tribunal ad quem las cuestiones referidas a la ubicación de tales datos, o que sea necesaria para efectuar dicho acceso, la inclusión de usuario y contraseña o no lo sea.

[578] Curso "Medidas de investigación tecnológica y evidencias digitales en la reforma de la Ley de Enjuiciamiento Criminal" de junio de 2016, realizadas en Alcalá de Henares, bajo el auspicio del Magistrado D. Joaquin DELGADO MARTÍN (Pág. 6, punto 5.4), existe un parecer completamente divergente como se extrae del Seminario sobre la nueva regulación de la LECrim en materia de investigación tecnológica realizado en Madrid año 2017 bajo el auspicio de DON JOSE MANUEL SÁNCHEZ SISCART en la que se concluye con la necesidad de recabar dicho auxilio (Pág. 69, punto 41 de las conclusiones).

III) El segundo gran grupo de autores son los que mantienen una posición que considera que el juez español carece de jurisdicción para ordenar el acceso y registro de los datos alojados en la nube cuando hay constancia de que los datos están fuera del territorio nacional.

Este grupo de autores se basa en la dicción de las leyes vigentes, y en especial el contenido del Convenio sobre Ciberdelincuencia de Budapest, fechado el 23 de noviembre de 2001 que se ha citado en varias ocasiones y el Convenio Europeo en materia de asistencia penal[579].

El art. 19 del Convenio de Budapest, ratificado por España, permite a los Estados firmantes adoptar medidas legislativas que implementen diligencias que faculten a acceder *«a un sistema informático o a una parte del mismo, así como a los datos informáticos almacenados en el mismo»*, o bien *«a un medio de almacenamiento de datos informáticos en el que puedan almacenarse datos informáticos».* El Convenio exige que esa información esté *«en su territorio»*, tal y como se dice en el apartado 2 del artículo, al exigir que *«los datos buscados están almacenados en otro sistema informático o en una parte del mismo situado en su territorio»*. El Convenio mantiene un principio de territorialidad ineludible, insoslayable e inexorable, que también se aprecia en el art. 20 del convenio, relativo a la obtención en tiempo real de datos de trafico. Además del contenido de estos convenios, estos autores recuerdan que la imposibilidad de realizar el acceso y registro fuera del territorio nacional está reconocida por instrumentos internacionales que han abordado la transferencia internacional de datos[580], o por organismos que se han referido a la cuestión concreta de la investigación delictiva[581]. Todos concluyeron que los datos que se pueden registrar son los que se encuentran en el interior del territorio, como ratifica expresamente el art. 19 del Convenio de

[579] Vid. ORTIZ PRADILLO, Juan Carlos. «Nuevas medidas tecnológicas de investigación criminal para la obtención de prueba electrónica» en ORTIZ PRADILLO, Juan Carlos. *El proceso penal en la sociedad de la información. Las nuevas tecnologías para probar el delito*. Editorial La Ley. Madrid. 2012. La Ley 7959/2012. Págs. 3 a 5.

[580] Cfr. DE MIGUEL ASENSIO, Pedro Alberto. «Aspectos internacionales de la protección de datos: las sentencias Schrems y Weltimmo del Tribunal de Justicia». *La Ley Unión Europea*, Nº 31, 30 de Noviembre de 2015. Pág. 4. Aunque el autor aborda la cuestión de transferencias internacionales de datos en general recuerda que: *«así como en el control de que las transferencias internacionales inherentes al funcionamiento de esos servicios no hacen posible el acceso a los datos por autoridades de terceros Estados sin las garantías adecuadas, como ha puesto de relieve nuevamente el Dictamen 02/2015 del llamado Grupo de Trabajo del art. 29 («Opinion 02/2015 on C- SIG Code of Conduct on Cloud Computing» de 22, de septiembre de 2015, págs. 6-8)»*.

[581] En el informe de la lucha contra la ciberdelincuencia 2017/2068 (INI) efectuada en la Comisión de Libertades Civiles, Justicia y Asuntos del Interior del Parlamento Europeo de fecha 25 de julio de 2017. Ponente: Elizabeth Vozemberg-Vridioni, se pone de manifiesto el aparente avance de las autoridades nacionales para acceder a datos ubicados fuera de su territorio. El punto 78 del documento sobre propuesta de resolución del Parlamento Europeo dice textualmente: «*78. Manifiesta su profunda preocupación por el trabajo en curso en el Comité del Convenio del Consejo de Europa sobre Ciberdelincuencia con respecto a la interpretación del artículo 32 del Convenio de Budapest en relación con el acceso transfronterizo a los datos informáticos almacenados («pruebas en la nube»), y se opone a la elaboración de un nuevo protocolo o directriz con vistas a ampliar el ámbito de aplicación de esta disposición más allá del régimen actual establecido por dicho Convenio —que ya constituye una excepción de calado al principio de territorialidad—, puesto que podría permitir que las fuerzas de seguridad gozaran de un acceso remoto ilimitado a los servidores y ordenadores ubicados en otras jurisdicciones, sin necesidad de recurrir a los acuerdos de asistencia judicial mutua ni a otros instrumentos de cooperación judicial establecidos para garantizar los derechos fundamentales de las personas, incluidas la protección de datos y las garantías procesales, como el Convenio n.º 108 del Consejo de Europa»;*

Budapest. De hecho, la única excepción a la prohibición de registro de datos situados fuera del territorio, está en el art. 32 del Convenio en la figura de los «*registros transfronterizos»*. Pero, en estos casos de registro más allá de las fronteras, será necesario acudir a los mecanismos de ayuda supranacional previstos en el art. 33 para cualquier otro registro de datos que se encuentren alojados fuera del territorio nacional.

La situación descrita lleva a estos autores a reclamar la creación de mecanismos expresos de cooperación judicial internacional sobre esta concreta materia[582]. Algunos otros estiman que lo que hay que desarrollar es el contenido del art. 32 del Convenio, que permite los registros de equipos situados fuera del territorio nacional, pero sólo cuando están en situaciones de proximidad muy concretas. De manera que la regulación de estos registros transfronterizos permitiría configurar un tipo de registro de repositorios de almacenamiento de datos en el extranjero fuera de los casos expresamente previstos en la actualidad en el art. 32 del Convenio[583].

IV) Por último hay otras posiciones doctrinales que consideran que la regulación actual no ofrece la habilitación jurisdiccional para registrar datos virtuales, y reclaman instrumentos eficaces para atajar esta situación, en particular, al considerar que no existe jurisdicción de los jueces españoles para registrar los datos que están más allá de nuestras fronteras[584].

Una vez expuestas la totalidad de posiciones doctrinales sobre el registro de datos en la nube, puede concluirse que, pese a que las opciones que se muestran a favor de reconocer jurisdicción al juez nacional para registrar datos en la nube, son las que muestran un mayor esfuerzo argumental, en realidad, son las posiciones restrictivas las que parecen más ajustadas a la situación legislativa en estos momentos.

La razón para concluir así es que las leyes vigentes no permiten el registro de datos fuera del territorio, y en el caso específico de la regulación de la LECrim, pese a que el factor territorial es claramente obviado, en realidad hace depender la realización efectiva del registro de la posibilidad de un acceso a dichos datos tan sencillo como improbable, en la medida en que se confía la efectividad del registro a que se disponga del usuario y la contraseña, o bien se cuente con una accesibilidad a los datos que, como expresión, no queda explicada ni definida, dejando claramente un vacío sobre tales formas de realizar el registro de los datos alojados en la nube. Esta ausencia de legislación impone aplicar a la práctica de la diligencia de registro de datos en la nube lo dispuesto

[582] Vid. MARTÍN MARTÍN DE LA ESCALERA, A,M. Op. Cit. Pág. 20.
[583] Vid. DELGADO MARTÍN, Joaquin. «La prueba electrónica en el proceso penal». *Diario La Ley*, Nº 8167, 10 de Octubre de 2013. La Ley 7336/2013. Pág. 8.
[584] Vid. DELGADO MARTÍN, Joaquin. *Investigación tecnológica y prueba digital en todas las jurisdicciones*. Editorial la Ley-Wolter Kluwer. Madrid. 2016. Pág. 495.

en el art. 19 del Convenio de Budapest que, no olvidemos, expresamente prohíbe el registro virtual si los datos están fuera del territorio del país que investiga.

La ausencia de datos en la memoria del ordenador, la negativa del investigado a facilitar el acceso y la falta de presencia en España de la entidad mercantil que custodie los datos, sólo deja al juez instructor la opción de acudir a los mecanismos de cooperación judicial internacional[585].

A mayor abundamiento, resulta relevante que las normas europeas que regulan estas formas de cooperación, y que se analizarán detalladamente más adelante, sean posteriores a la reforma de la LECrim de 2015 y que pese a ello España, al ratificar su contenido, resulte comprometida, en el caso en que ello sea necesario, a solicitar medidas de investigación, que incluyen las de investigación tecnológica relacionadas con el registro de datos, mediante el empleo de la orden de investigación europea, lo que prácticamente permite deducir el reconocimiento de que la legislación procesal no admite claramente la jurisdicción del Juez español para hacerlo sin acudir a dichas vías.

De este modo partiendo de un auto dictado en España, se deja en manos de jueces extranjeros la realización de la diligencia oportuna, y la posterior remisión de su resultado a España para poder analizarla e incorporarla a la causa. Se trata de la opción menos deseable y la más contradictoria con la naturaleza electrónica de una investigación que admite la ficción de tener los datos al alcance de la mano. Además, parece incluso contradictoria con la propia alocución contenida en la ley referente a que «*los datos estén disponibles desde España*», lo que añade una mayor confusión sobre la práctica de un registro que queda descartado por la localización de los datos.

La opción más restrictiva, para terminar, parece ser la más respetuosa con la protección de los derechos fundamentales, que es la razón de ser de esta reforma procesal, y además es la que parece asegurar menos controversia por la vía de los recursos. Por consiguiente, el modo más seguro de realizar este registro, desde una óptica que valore la legalidad y validez de la diligencia, es realizar el registro de datos a través de los mecanismos de ayuda judicial internacional que sean de aplicación[586].

[585] En apartados siguientes de esta tesis se estudiarán algunos de los procedimientos fijados en las leyes para iniciar, desarrollar y obtener diferentes formas de cooperación judicial internacional. En todo caso, es importante reseñar el contenido de la Directiva 2014/41/CE del Parlamento Europeo y del Consejo, de 3 de abril de 2014, relativa a la orden de investigación en materia penal, que ha sido traspuesta al ordenamiento español mediante la Ley 3/2018, de 11 de junio que reforma a su vez la Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la Unión Europea.

[586] En el BOE de 1 de junio de 2018 se ha publicado la ratificación por parte de España del Segundo Protocolo Adicional al Convenio europeo de asistencia judicial en materia penal, hecho en Estrasburgo el 8 de noviembre de 2001.

5.3.3. Mecanismos de cooperación judicial y otros métodos de auxilio judicial.

La instrucción penal es la fase de investigación de los hechos en la que se trata de buscar indicios que acrediten la comisión del ilícito penal [587], siendo posible que estos indicios estén fuera del territorio nacional.

Existen delitos especialmente proclives a originarse en el territorio de un país para consumarse en otro: terrorismo, blanqueo de capitales, etc. Además, la actual delincuencia, especialmente la organizada, se aprovecha del uso de la tecnología para sus fines, empleando smartphones, ordenadores, servicios en la nube, y cualquier medio que sirva para dispersar su actividad e impedir su localización. Esta supraterritorialidad en la comisión delictiva aconseja un mayor intercambio de información y una mejora de los medios técnicos y legales que permitan una colaboración rápida y sobre todo efectiva, tanto a nivel policial como judicial.

La utilidad de la cooperación judicial internacional lleva a realizar una exposición sobre los diferentes instrumentos de cooperación judicial contenidos en la LECrim, así como en otros textos normativos, sobre todo los que están orientados a permitir especialmente el registro de datos electrónicos en la nube, que es el objeto específico de esta parte del trabajo.

Los mecanismos de cooperación judicial internacional son herramientas legalmente establecidas y puestas a disposición del Juez instructor, que le permiten dirigirse a los jueces de otros Estados para obtener su ayuda. La razón para recabar este auxilio se debe a que la jurisdicción del juez nacional no alcanza hasta el lugar en el que están los indicios del delito investigado. sistemas de seguimiento que faciliten y alcancen su efectiva finalidad.

La LECrim contiene en el Título VIII alguna regulación sobre esta materia. En especial, ha de hacerse alguna consideración respecto de los arts. 183, 187 y 193 LECrim. El primer precepto contiene una referencia general al deber de cooperación y auxilio entre órganos jurisdiccionales; el segundo artículo exige que la forma que deba adoptar la petición de auxilio a órganos que no sean jurisdiccionales sea la de oficio; por último, el art. 193 LECrim regula la cooperación judicial prestada por órganos judiciales extranjeros.

Esta última forma de auxilio al juez es la que va a ser objeto de análisis en este apartado, porque es la más útil para conseguir la práctica de las diligencias de investigación que están siendo objeto de estudio en la presente tesis. El punto de partida está en la ayuda que se necesita para realizar la

[587] En el art. 13 LECrim. se establece que entre las labores de instrucción se encuentra la de consignar las pruebas del delito, recoger y poner en custodia lo que fuera necesario, identificar al delincuente, detener a los responsables, proteger a los perjudicados y medidas relacionadas con estas actividades que fueran necesarias.

diligencia que debe practicarse fuera de España, porque cuando se realiza dentro del territorio nacional el sistema de auxilio es la remisión de un exhorto al lugar en el que debe realizarse la práctica de tal diligencia.

En materia de cooperación internacional, la ley nacional se remite a los tratados internacionales y a las normas de la Unión Europea que resulten de aplicación [588]. Al respecto, debe tenerse en cuenta que resulta muy destacable también el incremento de las herramientas puestas a disposición de los órganos jurisdiccionales españoles para investigar delitos fuera de España, siendo una de las razones de este aumento, la pertenencia de España a la Unión Europea, ya que dentro de este ámbito político territorial se aprecia una mayor variedad de instrumentos con esa finalidad [589].

En esta línea, el Acuerdo de 27 de septiembre de 2018, del Pleno del Consejo General del Poder Judicial en el que se aprueba el Reglamento 1/2018, sobre auxilio judicial internacional y redes de cooperación judicial internacional constituye un ejemplo de este desarrollo. Se trata de una norma que centraliza y homologa los procesos de coordinación en esta materia. La Exposición de Motivos explica que se centraliza, por primera vez en una norma, una completa relación de todas las normas que hay sobre cooperación judicial internacional. En este sentido, el Reglamento 1/2018, para cumplir con estas funciones, crea el Servicio de Relaciones Internacionales del Consejo General del Poder Judicial, que es el órgano que brinda una asistencia efectiva a los jueces para que las solicitudes de cooperación judicial internacional tengan éxito. Este Servicio realiza las peticiones de ayuda y también recaba información al país a la que se haya cursado la misma para ver cuál es su estado.

En lo que se refiere a las normas de la Unión Europea debe destacarse la creación de un *«espacio público común de la Unión»*[590], lo que ha llevado a los países que lo integran a dar los pasos tendentes a una confluencia legislativa. Este Espacio común de libertad, justicia y seguridad

[588] En el ámbito de la Unión Europea había que acudir al Convenio de 29 de mayo de 2000, relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea; aunque a partir del 22 de mayo de 2017, es aplicable la Orden Europea de Investigación Penal (Directiva 2014/41/CE) una vez que se haya producido la implementación de dicha Directiva. También resultan de aplicación los instrumentos previstos en términos generales para la cooperación judicial internacional que se encuentran regulados en la Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la Unión Europea; destacando la orden europea de embargo preventivo de bienes o aseguramiento de pruebas en relación con la conservación rápida de datos, así como el exhorto europeo de obtención de pruebas. Cuando estemos ante situaciones que son ajenas al ámbito de la UE resultará de aplicación el Convenio sobre la Ciberdelincuencia, acordado en Budapest el 23-11- 2001 (ratificado por España BOE 17-9-2010), que a los efectos de este estudio permite solicitar medidas provisionales, remisión de datos, acceso transfronterizo a datos, y obtención en tiempo real tanto de datos asociados al tráfico como del contenido de las comunicaciones.

[589] El Reglamento 1/2018, sobre auxilio judicial internacional y redes de cooperación judicial internacional, pone de manifiesto en su Exposición de Motivos el carácter disperso e insuficiente de las normas sobre cooperación.

[590] Cfr. HOYOS SANCHO, Montserrat. «Armonización de los procesos penales, reconocimiento mutuo y garantías esenciales», en HOYOS SANCHO, Montserrat (Coord). *El proceso penal en la Unión Europea: garantías esenciales.* Instituto de Estudios Europeos, Lex Nova. Valladolid. 2008. Pág. 41 y ss.

configura una zona donde la coexistencia de normativas similares permita una adecuada y eficaz atención a los problemas que se plantean ante una investigación penal que trasciende a una sola nación.

Esta finalidad se materializa mediante la creación de instrumentos de cooperación, entre los que destacan el reconocimiento mutuo de resoluciones judiciales[591], basado en el principio de «*confianza mutua»*; la preeminencia del Derecho de la Unión jerarquizando las normas si éstas faltan, o renovando el Derecho existente sobre el particular[592]; la creación de organismos comunes encargados de la persecución de actos ilícitos[593]; el reconocimiento del modo de tramitar una determinada materia[594].

En suma, hay una serie importante de herramientas que permiten una efectiva y real cooperación entre órganos jurisdiccionales de los diversos Estados de la UE[595]. Además, no debe perderse de vista que no se trata sólo de prestar dicha cooperación judicial internacional, sino que se está avanzando hacia una auténtica integración que permita reconocer hechos y ejecutar resoluciones dictadas por otro Estado miembro, en la confianza de que el proceso respeta todos los derechos fundamentales reconocidos a nivel del Derecho de la Unión Europea. Estas herramientas pueden ser de diversos tipos, en concreto puede hablarse de tres clases: instrumentos legislativos, creación de organismos de enlace y coordinación, y instrumentos de soporte, consulta y ayuda.

Entre los medios legislativos, destaca, como herramienta de colaboración en el ámbito europeo, la orden europea de detención y entrega[596]. Es una figura que permite a cualquier autoridad judicial de la Unión, ordenar la búsqueda y detención de cualquier investigado, siempre que se den los

[591] Sobre reconocimiento mutuo de resoluciones judiciales cabe citar la Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la Unión Europea.

[592] La reciente Ley 29/2015, de 30 de julio, de cooperación jurídica internacional en materia civil, recoge expresamente la preeminencia del derecho europeo y sienta en su exposición de motivos que *«dentro de un complejo marco de relaciones internacionales con numerosos tratados y acuerdos internacionales en vigor, y numerosas disposiciones de la Unión Europea una Ley de cooperación jurídica internacional interna debe tener un carácter subsidiario. Dicho carácter se pone de manifiesto en el artículo 2.a) que, en virtud del principio de primacía del Derecho de la Unión, da prioridad a la aplicación en esta materia de las normas de la Unión Europea y de los tratados y acuerdos internacionales en los que España sea parte»*.

[593] Para poder observar la creciente importancia que va tomando el Espacio común de Libertad, Seguridad y Justicia del que venimos hablando podremos ejemplificar el avance con el contenido del Reglamento (UE) 2017/1939 del Consejo de 12 de octubre de 2017, por el que se establece una cooperación reforzada para la creación de la Fiscalía Europea.

[594] Vid. DELGADO MARTÍN, Joaquin. «El juez en la construcción del espacio judicial europeo. Instrumentos de apoyo al auxilio judicial entre estados miembros de la Unión Europea», en HOYOS SANCHO, Montserrat (Coord). *El proceso penal en la Unión Europea: garantías esenciales*. Instituto de Estudios Europeos, Lex Nova. Valladolid. 2008. Pág. 248 y ss.

[595] Algunas de las medidas que se citan en este apartado son sistematizadas en Vid. DELGADO MARTÍN, Joaquin en HOYOS SANCHO (Coord). *El proceso penal en la Unión Europea: garantías esenciales* Op. Cit. Págs. 258 a 262. Parte del orden seguido es el mismo que ha seguido este autor.

[596] La regulación de la materia descansa en la Ley 3/2003, de 14 de marzo, sobre la orden europea de detención y entrega.

requisitos necesarios para ello, y se respeten las garantías esenciales que actúan como mecanismo de limitación de su concesión[597].

En esta línea también ha sido relevante, durante un tiempo, la figura del exhorto europeo de prueba[598]. Es un instrumento de cooperación judicial internacional, que al igual que los exhortos entre organismos judiciales nacionales, sirve para recabar de un órgano judicial de otro Estado miembro de la UE la práctica de diligencias de investigación determinadas[599].

La actual regulación sobre esta materia se contiene en la Directiva 2014/41/CE del Parlamento Europeo y del Consejo de 3 de abril de 2014, relativa a la orden europea de investigación en materia penal, que cambia la denominación de exhorto europeo por la de orden europea de investigación (en adelante OEI), y con ella se amplían los instrumentos que permiten el desarrollo de la investigación criminal fuera de las fronteras de cada país miembro.

La orden de investigación permite que la autoridad judicial que lo necesite (la llamada Autoridad de emisión), solicite que se realicen concretas diligencias de investigación previstas en la legislación nacional, pero que, en lugar de ser llevadas a cabo por la solicitante, sean ejecutadas por un organismo judicial de otro Estado miembro que se denomina Autoridad de ejecución.

La regulación de la Directiva sobre la orden europea de investigación debió trasponerse a la ley española antes del 22 de mayo de 2017[600], y aunque dicha trasposición no se realizó en las fechas establecidas, finalmente la Ley 3/2018, de 11 de junio, por la que se modifica la Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la Unión Europea, para regular la Orden Europea de investigación, ha sido la encargada de realizar dicha trasposición.

Era tanta la necesidad de aplicar esta Directiva, que durante el periodo que transcurrió desde que debió ser traspuesta, hasta que finalmente lo fue, existieron distintos pareceres que defendieron su inmediata aplicación[601], llegando a darse directrices sobre su tratamiento y consideración[602].

---

[597] Vid. JIMENO BULNES, Mar. «Orden europea de detención y entrega: garantías esenciales» en HOYOS SANCHO, Montserrat (Coord). *El proceso penal en la Unión Europea: garantías esenciales*. Instituto de Estudios Europeos, Lex Nova. Valladolid. 2008. Pág. 106 y ss. En el mencionado estudio aborda, entre otros aspectos, la excepción introducida al principio de doble incriminación, tradicionalmente establecido como un límite a la extradición, pero que se ha visto un tanto suavizado, sobre todo para la persecución de determinados delitos especialmente graves.

[598] Vid. DE LUCAS MARTÍN, Ignacio. «La prueba en el proceso penal en el contexto de la Unión Europea» en HOYOS SANCHO, Montserrat (Coord). *El proceso penal en la Unión Europea: garantías esenciales*. Instituto de Estudios Europeos, Lex Nova. Valladolid. 2008. Pág. 426 a 431.

[599] La figura de exhorto europeo de prueba sólo servía, hasta ese momento, para recabar pruebas que ya se habían practicado y que resultaban útiles en otro proceso abierto por otro Estado miembro, estando muy limitados los casos en los que se podía utilizar.

[600] Art. 36.3 de la Directiva 2014/41/CE.

[601] Vid. TRENADO SEARA, Javier. «La ineficaz Orden Europea de Investigación en materia penal». *Revista Electrónica Abogacía Española*. 10 de noviembre de 2017. (http://www.abogacia.es/2017/11/10/la-ineficaz-orden-europea-de-investigacion-en-materia-penal/).

Siguiendo las palabras de la Exposición de Motivos, esta norma se promulga *« a efectos de obtener una o varias medidas de investigación específicas que se llevarán a cabo en el Estado de ejecución de la misma, con vistas a la obtención de pruebas o a recabar las que ya están en posesión de la autoridad de ejecución*»[603]. La Ley 22/2014, ha visto reformado por completo su Título X, con la finalidad de regular la OEI[604], que sigue los principios y exigencias determinados por la Directiva.

Las autoridades españolas que reciban este tipo de órdenes examinarán y apreciarán si pueden llevarla a cabo conforme a la propia legislación interna[605]. La ley española prevé que mediante esta orden se pueda solicitar la realización de todas las diligencias necesarias, si bien la práctica de una diligencia debe obedecer a una verdadera necesidad para el Estado que la solicita, pues siguiendo el Considerando undécimo, *«la autoridad de emisión debe asegurarse, por consiguiente, de que la prueba buscada sea necesaria y proporcionada para el procedimiento, de que la medida de investigación escogida sea necesaria y proporcionada para obtener la prueba en cuestión, y de si procede implicar a otro Estado miembro en la obtención de dicha prueba por medio de la emisión de una OEI»* .

La amplitud con la que se ha redactado nuestra legislación interna, permite, que cualquier Estado que solicite una OIE, pueda valerse de la diligencia de registro de datos que está permitida en nuestra legislación procesal. De manera que, conforme a los criterios establecidos por las normas que regulan esta diligencia se valorará esta petición. En este sentido, no debe perderse de vista que lo mismo sucede para las diligencias de investigación que afectan a las comunicaciones y que se hayan exigido también en el curso de una investigación tecnológica [606].

---

[602] Muestra de lo que se dice es el contenido del dictamen emitido por la Unidad de Cooperación Internacional de la Fiscalía General del Estado sobre el régimen legal aplicable debido a la no trasposición en plazo de la orden europea de investigación y sobre el significado de la expresión "disposiciones correspondientes" que sustituye dicha directiva. Dicho dictamen está fechado el 19 de mayo de 2017. De ella cabe destacar fundamentalmente la decisión de seguir considerando las OEI como solicitudes internaciones de cooperación tradicionales.

[603] Así se indica en el apartado II, párrafo tercero de la Exposición de Motivos.

[604] La norma define esta Orden en su art. 186.1 como *«una resolución penal emitida o validada por la autoridad competente de un Estado miembro de la Unión Europea, dictada con vistas a la realización de una o varias medidas de investigación en otro Estado miembro, cuyo objetivo es la obtención de pruebas para su uso en un proceso penal. También se podrá emitir una orden europea de investigación con vistas a la remisión de pruebas o de diligencias de investigación que ya obren en poder de las autoridades competentes del Estado miembro de ejecución»*

[605] El apartado segundo del párrafo primero del art 186 dice sobre este aspecto que *«Se considerarán válidos en España los actos de investigación realizados por el Estado de ejecución, siempre que no contradigan los principios fundamentales del ordenamiento jurídico español ni resulten contrarios a las garantías procesales reconocidas en éste.»*

[606] El Considerando 30 de la Directiva expresamente incluye los datos relativos a comunicaciones: «*Las posibilidades de cooperación, conforme a lo establecido en la presente Directiva, en materia de intervención de las telecomunicaciones no deben limitarse al contenido de la comunicación, sino que pueden abarcar igualmente la obtención de datos de tráfico y localización correspondiente a tales comunicaciones, lo que permitirá a las autoridades competentes emitir una OEI con vistas a la obtención de datos de telecomunicaciones con menos intrusión en la vida privada. Una OEI emitida con el fin de obtener datos históricos de tráfico y de localización de las telecomunicaciones*

La petición formal de la práctica de una OIE se formulará por cualquier medio que permita dejar constancia de la solicitud, inclusive el empleo de la Red Judicial Europea, y se verificará usando el modelo normativizado contenido en el Anexo XIII de la Ley, en lo que se refiere a su expedición, y el Anexo XIV para confirmar su recepción, en el caso de ser el país receptor. Una vez recibido, la autoridad del país encargado de ejecutarla examinará su procedencia y su valoración, conforme a los principios de necesidad y de proporcionalidad, y analizará, si conforme a su propia legislación, cabe llevar a cabo la práctica de estas diligencias, y si sería procedente llevarla a cabo, conforme al derecho interno propio, en un caso similar[607]. En el caso que la legislación nacional de la autoridad de ejecución no contemple la diligencia interesada se puede optar por ejecutar una medida similar[608], prevista en dichas leyes. Además, debe tratarse de una diligencia que sea susceptible de poder ejecutarse en el tipo penal que está siendo investigado[609].

Los principios sobre los que pivota la eficacia y utilidad de la OEI son la coordinación y la rapidez, lo que ha sido plasmado y recogido también en la Ley española. Para hacer efectivos estos principios se exige del órgano encargado de la ejecución acusar recibo y mantener al órgano de emisión constantemente informado de la ejecución de la medida, además de poner a disposición del órgano emisor el contendido de la diligencia una vez practicada[610].

La petición de ayuda se puede denegar y con ello desestimar la práctica de la diligencia interesada mediante una orden europea de investigación [611], pero hay casos en que esto no es posible. Así expresamente viene previsto en la Directiva y en la Ley española [612] que indican que no podrá denegarse la petición que consista en *«la obtención de información contenida en bases de datos que obren en poder de las autoridades policiales o judiciales y que sean directamente accesibles a la autoridad de ejecución en el marco de un procedimiento penal».* En suma, puede decirse que esta Ley se convierte en una norma trascendental a aplicar cuando se sepa que el dato o archivo objeto

---

debe tratarse con arreglo al régimen general de ejecución de la OEI, y podrá considerarse, en función del Derecho nacional del Estado de ejecución, como una medida de investigación coercitiva».

[607] Ver Art. 6.1.b) de la Directiva, y plasmada en la Ley 22/2014 en su artículo 186.1.

[608] Ver Art. 10.1, apartados a y b de la Directiva, y el art. 206.2 de la Ley 22/14, que dispone «*2. Cuando el resultado perseguido por la orden europea de investigación pudiera conseguirse mediante una medida de investigación menos restrictiva de los derechos fundamentales que la solicitada en la orden europea de investigación, la autoridad competente española ordenará la ejecución de esta última»*. Los apartados 3 y 4 de este mismo artículo permiten que se ordene una diligencia distinta que permita conseguir un resultado similar, para lo que debe informarse a la autoridad solicitante, por si quiere modificar, dejar sin efecto o permitir la práctica de la diligencia alternativa.

[609] Esto implicaría que, por ejemplo, si se interesa por la Autoridad emisora un registro remoto de equipo electrónico, diligencia que nuestra legislación procesal admite, sólo podrá acordarse para investigar los delitos que se contemplan en el art. 588 septies a, 1 LECrim española. Por lo tanto, si es para investigar otros delitos, debe rechazarse el reconocimiento de la petición.

[610] Ver Arts. 13 y 16 de la Directiva y artículo 208 de la Ley 22/2014, que es el que recoge el procedimiento de reconocimiento de las peticiones de OIE..

[611] La denegación de la practica de la diligencia se prevé y se regula expresamente en el art. 11 de la Directiva y se desarrolla en el art. 207 de la Ley 22/2014..

[612] Ver Art. 10.2. b) de la Directiva y artículo 206.1 de la Ley 22/2014..

de búsqueda esté en algún servicio en la nube ubicado dentro de la UE. La autoridad de ejecución no podrá negar el acceso a la base de datos alojada en su territorio porque a tal autoridad le es accesible, siendo la única razón por la que podría denegar la medida sería que dicha diligencia de acceso a los datos no existiese en su derecho interno.

En lo que se refiere al resto de países no integrantes de la UE habrá que estar al contenido de los diferentes acuerdos internacionales suscrito sobre el particular.

El segundo grupo de instrumentos de cooperación internacional en la investigación penal está constituido por organismos encargados de coordinar o enlazar las actividades judiciales. Nuevamente es en el ámbito de la UE donde estas medidas se han implementado de un modo más intenso, y donde surten más efecto, pero existen también en otros marcos internacionales. Estos organismos son impulsados por un espíritu de colaboración, y persiguen la finalidad de evitar la indeseada lentitud en la respuesta judicial, ya que esta demora es incompatible con el derecho a obtener la tutela judicial efectiva en plazos razonables, lo que se concreta en la evitación de dilaciones indebidas[613]. La línea procesal actual trata de impulsar, con esta misma intención, una mayor agilidad del proceso penal regulando nuevas diligencias de investigación más rápidas o reduciendo los plazos de la instrucción penal[614].

La primera figura que se puede destacar entre los organismos de coordinación, es la del magistrado de enlace[615], que son los jueces y magistrados nacionales que, dispuestos en los países en los que se decide ubicarlos, son encargados de acelerar el proceso de finalización de diligencias, impulsar ante la autoridad judicial extranjera su realización, así como realizar labores de coordinación con el organismo Eurojust[616]. Esta figura permite, mediante un acceso telefónico o mediante correo electrónico directo, consultar las dudas sobre el proceso del país receptor de la petición, así como

[613] Ver sobre el particular la STC 77/2016, de 25 de abril. Ponente: Don Pedro González-Trevijano Sánchez. Aunque la sentencia viene referida al ámbito de lo contencioso administrativo, su análisis de las dilaciones indebidas es extrapolarle a cualquier orden jurisdiccional. La resolución termina concediendo el amparo al considerar vulnerado el derecho contenido en el art. 24.2 del texto constitucional.

[614] La nueva redacción conferida por la Ley 41/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para la agilización de la justicia penal y el fortalecimiento de las garantías procesales, al contenido del art. 324 de la LECrim, ha supuesto una fijación de plazos de instrucción criminal que ha sido objeto de numerosos análisis, dado que ello incide en la situación procesal en la que queda la causa una vez transcurridos los mismos. Puede consultarse de manera breve el trabajo de Vid. RIVERA HERNÁNDEZ, José María. «El análisis del artículo 324 de la Ley de Enjuiciamiento criminal». Dicho trabajo fue expuesto en los cursos de formación para Fiscales ofrecidos el día 30 de marzo de 2016 denominados Los nuevos Plazos de Instrucción, 1º edición. El contenido del trabajo puede leerse en el siguiente
enlace:https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20Rivera%20Hernández,%20José%20Mª.pdf?idFile=96cb7f42-7030-4b6f-b9ac-d454edef5c52.

[615] Se insiste en que sigue el mismo orden fijado en el trabajo antes aludido de DELGADO MARTÍN, Joaquin en HOYOS SANCHO (Coord). *El proceso penal en la Unión Europea: garantías esenciales* Op. Cit. Págs. 258 a 262.

[616] En el caso de España, la Ley 16/2015, de 15 de julio, regula el estatuto jurídico del miembro de nacional de España en Eurojust, los conflictos de jurisdicción, las redes judiciales de cooperación internacional y el personal dependiente del Ministerio de Justicia en el exterior.

realizar labores de puesta al día de su realización. El acceso al magistrado de enlace[617] se realiza de manera interna, entre los Jueces y Tribunales, siendo aquel magistrado el que informa y realiza actividades tendentes a solventar los problemas derivados de la interactuación de diferentes ordenamientos jurídicos.

La oficina Eurojust ya mencionada, es otro de estos organismos de coordinación entre países de la UE, y también ha ido adquiriendo con el tiempo mayor importancia, notoriedad y efectividad en sus cometidos[618]. Sirve como oficina coordinadora de la investigación penal entre los países miembros de su estructura[619] , y permite coordinar a varias autoridades judiciales, miembros de la UE, para que la investigación alcance un fin adecuado. Además se encarga de cumplir con una importante función de resolución de los problemas y conflictos de jurisdicción que se originan cuando dos o más países integrantes de su estructura investigan delitos que se cometen indistintamente en el interior del territorio de cada uno de ellos. A todo ello se une su función de coordinar las órdenes de detención que se expiden en países que lo integran.

La composición y funcionamiento de Eurojust están regulados por una normativa europea específica[620], y sus atribuciones pasan por la mejora activa y efectiva en la ordenación entre las autoridades encargadas de la investigación criminal de los países integrantes. Lleva a cabo reuniones en su sede, en las que se ponen en común, con los integrantes de los países afectados, los problemas de acoplamiento y coordinación entre organismos judiciales, se agiliza la entrega de diligencias practicadas a instancias de la autoridad judicial de un país por otro o se ponen en común los resultados de múltiples actuaciones conjuntas[621]. En este sentido los representantes de cada país en Eurojust velan porque se entreguen los documentos solicitados por otros países, ayudan cuando existe alguna duda o dificultad, y coordinan actividades en los que participan autoridades policiales y judiciales de varios Estados miembros.

---

[617] El proceso de selección de los Magistrados de Enlace se regula en el Real Decreto 242/2019, de 5 de abril, por el que se regula el régimen jurídico del personal del Ministerio de Justicia que lleva a cabo la acción en el exterior en materia de justicia.

[618] Eurojust, fue creada en virtud de la Decisión 2002/187/JAI, del Consejo, de 28 de febrero de 2002, por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia.

[619] El Reglamento (UE) 2017/1939 del Consejo de 12 de octubre de 2017, por el que se establece una cooperación reforzada para la creación de la Fiscalía Europea, parte de las actuales funciones de la oficina Eurojust como germen de la futura Fiscalía.

[620] La oficina Eurojust fue creada por la Decisión 2002/187/JAI del Consejo de 28 de febrero de 2002 por la que se crea Eurojust para reforzar la luchas contra las formas graves de delincuencia. Dicha decisión fue modificada por la decisión 2003/259/JAI del Consejo por la que se modifica la decisión 2002/187/JAI del Consejo de 28 de febrero de 2002. Su última modificación es la decisión 2009/426/JAI del Consejo de 16 de diciembre de 2008 por la que se refuerza Eurojust.

[621] Todas estas funciones pueden consultarse en su web: http://www.eurojust.europa.eu/Pages/languages/es.aspx. En el apartado de funciones cabe destacar, como se ha dicho que *«Las reuniones de coordinación se centran en casos concretos, en relación a los delitos considerados como prioritarios por el Consejo de la Unión Europea: terrorismo, narcotráfico, tráfico de seres humanos, fraude, corrupción, delito informático, blanqueo de capitales y otras actividades ilegales relacionadas con la presencia de grupos delictivos organizados en la economía»*.

La nueva Fiscalía Europea, de la que ya se han realizado algunas consideraciones sobre sus competencias y funciones a lo largo del desarrollo de este trabajo, y a las que cabe remitirse en aras de evitar reiteraciones que alarguen este estudio, es otro de los organismos que sirven para tratar de manera conjunta y coordinada, las actividades de investigación penal, si bien, como se tuvo ocasión de señalar, circunscrita a ámbitos delictivos muy concretos.

Junto al ámbito amparado por las instituciones europeas, hay otros sectores de actuación en los que también se ha avanzado en esta coordinación, destacando la figura de la Red Judicial Europea[622], y la Red Judicial Española de Cooperación Judicial Internacional[623], e Ibered en el espacio iberoamericano[624]. Son tres organizaciones que sirven de ejemplo de colaboración judicial mutua entre los diversos países que las integran. Persiguen el fomento de la efectividad de sus labores propias, cuando se necesita la colaboración territorial externa. Así la función primordial de la Red Judicial Europea es la de *«facilitar la cooperación judicial entre los Estados miembros, en particular en la actuación contra las formas de delincuencia grave»*[625], para ello sus normas reguladoras crean una serie de puntos diseminados por el territorio de dicha red, compuesto por jueces y magistrados, que tienen por actividad principal el suministro de información básica, la actualización de la misma y la realización de reuniones de coordinación. Las funciones de la Red Española de Cooperación Judicial Internacional, a diferencia de la red europea, están dirigidas a dar *«cumplimiento a las solicitudes de auxilio judicial provenientes de otros Estados en la forma prevista en la Ley Orgánica del Poder Judicial, en las leyes especiales y en el presente Reglamento, así como en los Tratados y Convenios Internacionales de los que España sea parte y en las normas de la Unión Europea que resulten aplicables»*[626].

Por último, Ibered, tiene por finalidad según su propio estatuto regulador *«optimizar la cooperación judicial en materia penal y civil entre los países participantes en la Comunidad Iberoamericana de naciones….y establecer progresivamente y mantener actualizado un sistema de información sobre los diferentes sistemas legales de la Comunidad Iberoamericana de Naciones»*[627].

[622] Esta Red fue creada por la Acción Común de 29 de junio de 1998, adoptada por el Consejo, sobre la base del artículo K.3 del Tratado de la Unión Europea, por la que se crea una red judicial europea.
[623] Esta Red se regula mediante el Reglamento 1/2018, de 27 de septiembre, sobre auxilio judicial internacional y redes de cooperación judicial internacional.
[624] Puede consultarse en su página web: https://www.iberred.org el conjunto de funciones de esta institución, pero en todo caso cabe dejar apuntado que la finalidad perseguida con esta institución, al igual que otras que se han esbozado en esta parte de esta investigación, es la de fomentar la mejora de la coordinación entre las autoridades judiciales de cada país integrante.
[625] Ver Titulo II, artículo 4.1 de la Acción Común.
[626] Art.1.1 del Reglamento 1/2018, de 27 de septiembre, sobre auxilio judicial internacional y redes de cooperación judicial internacional.
[627] Disposición 3 del Título I del Reglamento de la Red Iberoamericana de Cooperación Jurídica Internacional, Iberred.

En tercer lugar, junto a las medidas legales y organizativas ya descritas, existen algunas otras herramientas de trabajo de carácter práctico que mejoran la actividad judicial internacional. Son sistemas de consulta y de resolución de dudas que permite a cada juez acudir a ellas para asegurar que realiza las acciones de petición fuera del territorio nacional, empleando los medios técnico-legales adecuados. Hay que destacar que suelen tomar forma de páginas o portales web, que, como otras bases de datos, permiten obtener información actualizada y útil. Una de estas herramientas es el Atlas Judicial Europeo, que se configura mediante una página web, que ofrece una información detallada y útil para saber cómo llevar a cabo diversas diligencias de investigación en países miembros de la unión europea. Además, incluye la misma información sobre naciones del mismo territorio que, sin ser parte de la unión europea, si conforman la red judicial[628].

También hay que hacer reseña del "Prontuario de Auxilio Judicial Internacional"[629], que se define como *«una herramienta facilitadora de las actividades de auxilio judicial internacional que está a disposición de todos los miembros de la carrera judicial, fiscal y del cuerpo de letrados de la administración de justicia»*. Adopta la forma de una página web dirigida a realizar consultas y que contiene información, sobre todo la normativa vigente, acerca del modo efectivo de llevar a cabo la diligencia que en cada caso interese practicar. En su contenido reúne todas las normas internacionales vigentes tanto en el entorno europeo, como el correspondiente a los demás países con los que España tiene suscrito alguna clase de convenio sobre cooperación judicial. Ofrece los datos de cada organismo judicial, e incluye los formularios de petición de cada una de las diligencias que resulten de interés. Estos modelos, en muchos casos, resultan de uso obligado, lo que fortalece y dar mayor seguridad jurídica al proceso. El Prontuario se divide entre la jurisdicción penal y la civil[630]. Es una herramienta muy útil ante lo complejo que es, en ocasiones, conocer el contenido de todos los tratados que España suscribe con terceros países en esta materia. Es

[628] En el enlace https://www.ejn-crimjust.europa.eu/ejn/AtlasChooseMeasure.aspx?Mp=0&Cou=373, pueden apreciare las distintas diligencias de carácter penal de las que el mencionado instrumento ofrece información. A título de ejemplo lo que ofrece el mencionado instrumento es la información de cómo proceder a realizar diligencias con cada uno de los países integrantes, como pudieran ser diligencias de interceptación, grabación y transcripción de comunicaciones, interceptación de correo, observación, etc. La finalidad es útil en la medida en que orienta a las distintas autoridades judiciales sobre cómo abordar cada cuestión.

[629] Se regula en el art. 3 del Reglamento 1/2018 de 27 de septiembre, sobre auxilio judicial internacional y redes de cooperación judicial internacional.

[630] Puede accederse a través del enlace http://www.prontuario.org/portal/site/prontuario. Debe recordarse que se trata de un instrumento de uso judicial y por ello está sometido a la obtención de un usuario y una contraseña que se facilita a las personas que ejercen las funciones judiciales y también a los miembros del Ministerio Fiscal. Hay que notar que muchos de sus formularios son de obligado uso y cumplimentación. Por ejemplo cabe citar la existencia de un formulario que previene de la posibilidad de solicitar lo que se conoce como exhorto europeo de obtención de pruebas a una autoridad judicial de otro estado miembro (ver enlace: http://prontuario.poderjudicial.es/prontuario/es/Penal/Formularios/ci.Certificado-para-la-ejecucion-de-exhorto-europeo-de-obtencion-de-pruebas.formato1?channels=3142651ca5fb6310VgnVCM1000006f48ac0a____&UE=si).

destacable[631] el ahorro de tiempo y esfuerzo para localizar la normativa aplicable, lo que convierte a esta herramienta en una importante base de datos en la que todos esos convenios están relacionados y sistematizados, y donde incluso están los modelos de petición normativizados.

6. El resultado de las diligencias de investigación tecnológica en el procedimiento. Medios de impugnación y la valoración de la prueba tecnológica.

Una vez expuesto el desarrollo de las diferentes diligencias de investigación de acceso y registro de datos, sus implicaciones en materia de derechos fundamentales y los especiales problemas que plantean los registros de datos en la nube, cabe adentrarse en el estudio del análisis jurídico-procesal del resultado obtenido como consecuencia de la ejecución de las diligencias de registros de datos electrónicos, llevadas a cabo siguiendo los arts. 588 sexies y 588 septies LECrim.

Con este fin se tratarán de forma sucesiva varias cuestiones: las formas de incorporación de los datos obtenidos en la práctica de las diligencias a la causa penal; los modos de impugnación de su ordenación, contenido y resultado por parte de las defensas y las acusaciones y, en tercer lugar, se tratará el mecanismo de valoración de estas diligencias en la fase de enjuiciamiento.

6.1. Aportación de los datos tras la práctica de las diligencias de investigación al procedimiento.

La petición de la práctica de las diligencias de registro de dispositivos electrónicos, en tanto que limitan alguno de los derechos del art. 18 CE, debe ser explicada y justificada por los que la solicitan. Por eso, el oficio policial en el que se realiza la petición de práctica de la medida debe reunir toda la información de la que se disponga sobre los hechos con trascendencia penal que se investigan, y las razones que conducen a solicitar estas concretas diligencias de investigación y no otras. Esta información detallará aspectos como: los datos de los que se disponga de las personas implicadas, las diligencias sin alcance limitador de derechos constitucionales ya efectuadas, como

[631] DELGADO MARTÍN, Joaquin en HOYOS SANCHO (Coord). *El proceso penal en la Unión Europea: garantías esenciales* Op. Cit. Págs. 258 a 262.

algún seguimiento directo[632], la información derivada de la consulta fichas policiales, y todo cuanto justifique la solicitud.

La admisión de esta solicitud por parte del Juzgado de Instrucción, en ocasiones, suele fijar el inicio formal de la instrucción de la causa, lo que se realiza con el auto correspondiente al que le sigue la resolución judicial sobre la pertinencia de la diligencia solicitada. En todo caso, a pesar del inicio formal que se le da a la investigación nada impide que a posteriori se archive o sobresea porque los hechos no revistan entidad delictiva o no se logre determinar el autor.

En cualquier caso, y centrándonos en las diligencias que se estudian en este trabajo, la propia naturaleza de éstas hará que en la práctica se comporten en la mayor parte de los casos como diligencias de investigación subsiguientes de otras, y que se practicarán dentro de un proceso penal ya iniciado. De hecho, en otras partes de este trabajo, dedicadas a la clasificación de las diligencias de registro de datos electrónicos, se ha destacado que las diligencias de acceso y registro de datos actuaban como diligencias de complemento, refuerzo, ampliación y detalle de otras previas.

Este carácter derivado se corrobora con la redacción del art. 588 sexies, apartado a LECrim, que coloca a estas diligencias como el resultado material de la práctica de una diligencia de entrada y registro en domicilio, lo que ya es una diligencia de investigación previa a la de registro de datos[633].

En resumen, puede decirse que las actividades de la policía judicial [634], sobre todo cuando éstas son de naturaleza propiamente investigadora[635], podrán ser el mecanismo de comunicación al juez

---

[632] Sobre este particular asunto resulta muy interesante el libro de Vid. MARTÍN MORALES, Joaquin. *El régimen constitucional del seguimiento directo de personas*. Comares. Granada. 2015. En especial en las páginas 12 y siguientes el autor destaca que ha de diferenciarse entre el seguimiento directo a personas, de aquel en el que se emplean medios tecnológicos para hacerlo. Analiza los derechos fundamentales implicados. Sin embargo, a los efectos de despejar dudas, el autor deja especificado (pág. 24, apartado. 6.1) que no hace falta autorización judicial para un mero seguimiento físico de la persona. Sigue el autor desarrollando y manteniendo el mismo criterio en las páginas 34 y 35.

[633] Este carácter derivado también se aprecia en el art. 588 sexies, apartado b LECrim, en la que el dispositivo se encuentra fuera de un domicilio, porque cabe colegir que para obtener dicho dispositivo en esas circunstancias también es necesario que concurra alguna diligencia anterior como un cacheo personal, o el registro de un vehículo, etc. El carácter de diligencia derivada también es predicable en el art. 588 septies apartado a LECrim. Al tratarse de una diligencia restringida a la investigación de concretos delitos, se puede estimar que lo más habitual en delitos del calado que se refleja en dicho artículo, es la existencia de una investigación ya iniciada sobre tales ilícitos, pero que para ser culminada exigen la practica de la intervención remota de un ordenador.

[634] Se trata de las normas que regulan los Cuerpos y Fuerzas de seguridad del Estado, que se compone en lo que aquí nos interesa en la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad. y en el Real Decreto 769/1987, de 19 de junio, sobre regulación de la Policía Judicial.

[635] Se destaca el contenido del art. 4 del RD 769/1987 a cuyo tenor «*Todos los componentes de las Fuerzas y Cuerpos de Seguridad, cualquiera que sean su naturaleza y dependencia, practicarán por su propia iniciativa y según sus respectivas atribuciones, las primeras diligencias de prevención y aseguramiento así que tengan noticia de la perpetración del hecho presuntamente delictivo, y la ocupación y custodia de los objetos que provinieren del delito o estuvieren relacionados con su ejecución, dando cuenta de todo ello en los términos legales a la Autoridad Judicial o Fiscal, directamente o a través de las Unidades Orgánicas de Policía Judicial*». A continuación, es el art. 28 el que se detiene en ofrecer numerosos ejemplos de las funciones a realizar entre las que hay que destacar: «*a) Inspecciones oculares. b) Aportación de primeros datos, averiguación de domicilios y paraderos y emisión de informes de solvencia o de conducta. c) Emisión, incluso verbal, de informes periciales provisionales, pero de urgente necesidad para adoptar decisiones judiciales que no admiten dilación. d) Intervención técnica en levantamiento de cadáveres. e)*

instructor de los hechos investigados y origen de subsiguientes actuaciones procesales cuando una vez puestas en conocimiento del juez instructor[636], éste ordene la realización de la diligencia y la unión de su resultado al proceso. Nada impide que junto con la concreta diligencia que se pida, se desarrollen muchas otras como seguimientos o interrogatorios.

La incorporación del resultado de las diligencias de investigación de datos no acaba con su unión a las actuaciones, sino que resulta necesario que sobre éstas diligencia se realice una interpretación de los datos encontrados con estas diligencias. Para lo cual, es preciso dejar constancia del proceso de extracción de la información derivada de la práctica de estas diligencias, así como del análisis de la misma, que es una actividad que tiene un elevado carácter técnico que exigirá la participación de expertos que hagan comprensibles estos datos tanto al juez como a las partes, para que los criben en aras a obtener sólo los que tienen interés para la investigación[637].

La doctrina científica considera que el resultado de las diligencias de investigación tecnológica puede tener la naturaleza de *«pruebas preconstituídas»* [638], pero, en este sentido, no debe perderse de vista que esta consideración como pruebas preconstituídas, aunque pueda haber existido una resolución judicial que valore las circunstancias concurrentes en el supuesto de hecho, y que adopte las garantías para la incorporación del resultado a las actuaciones con respeto a los derechos afectados[639], no las convierte en inatacables.

Recogida de pruebas. f) Actuaciones de inmediata intervención. g) Cualesquiera otras de similar naturaleza a las anteriores. h) Ejecución de órdenes inmediatas de Presidentes, Jueces y Fiscales». Como puede apreciarse los agentes cuentan con autonomía en el inicio de la actuación si bien han de recabar el seguimiento judicial en las diligencias que fueran a practicar.

[636] La doctrina tradicional ha venido considerando que la fase de instrucción tiene por finalidad esencial *«preparar el juicio oral»* y distingue como funciones propias de esta fase tres: *«la realización de las diligencias de investigación, la de adoptar las medidas cautelares penales, y la tercera consiste en adoptar las medidas cautelares civiles».* Cfr. GIMENO SENDRA. Vicente. *Derecho procesal penal.* Segunda edición. Thomson Reuters Civitas. Pamplona. 2015. Págs. 350 y 351. Como puede comprobarse la finalidad que se destaca en primer lugar es la investigadora por lo tanto es muy destacable que el legislador haya incluido una batería de diligencias que permitan un esclarecimiento completo de los hechos.

[637] Ciertamente las cuestiones referentes a los aspectos derivados del empleo de las tecnologías de la comunicación han sido muy polémicas, y sobre todo han estado muy mezcladas con relevantes aspectos relacionados con derechos fundamentales como el derecho a la prueba. Es lo que le sucedió al sistema SITEL como el empleado para captar y grabar conversaciones telefónicas, y en todo ello el TS optó finalmente por considerar en la mayor parte de las ocasiones innecesaria la práctica de periciales informáticas sobre el uso de dicho sistema por considerar su resultado como óptimo y seguro desde un punto de vista técnico para considerarse como prueba de cargo. STS 722/2012, de 2 de octubre. Ponente: D. Cándido Conde Pumpido y Tourón.

[638] Cfr. GIMENO SENDRA. Vicente. *Derecho procesal penal, segunda edición*. Op. Cit. pág. 547.

[639] La consideración de una prueba como preconstituida no sólo ha sido una categoría que se ha estudiado por la doctrina sino que conforma un nutrido cuerpo de doctrina constitucional. Así la STC 68/2010 de 18 octubre, ponente Doña Elisa Pérez Vera, citando a otras muchas del propio Tribunal viene a configurar los aspectos de los que depende considerar como preconstituida una determinada diligencia, indicando que se exige el *«cumplimiento de una serie de presupuestos y requisitos que hemos clasificado como: a) materiales –que exista una causa legítima que impida reproducir la declaración en el juicio oral–; b) subjetivos –la necesaria intervención del Juez de Instrucción–; c) objetivos –que se garantice la posibilidad de contradicción, para lo cual ha de haber sido convocado el Abogado del imputado, a fin de que pueda participar en el interrogatorio sumarial del testigo–; y d) formales –la introducción del contenido de la declaración sumarial a través de la lectura del acta en que se documenta, conforme a lo ordenado por*

El contenido de estas diligencias ha de ser sometido a contradicción, y por eso se admite que las defensas aporten pruebas que lo contradigan. Para ello, las pruebas que de forma más habitual se aportan son las periciales informáticas o técnicas que desmientan el contenido de los informes de los investigadores, introduciendo algún elemento de duda en práctica de la diligencia[640], como: la falta de aseguramiento en la cadena de custodia; el modo de ejecutarla; su fiabilidad; la cualificación profesional del autor del informe; la autenticidad de los datos: o el cuestionamiento de aspectos más formales [641] como el modo de examinar los datos encontrados en los dispositivos incautados o intervenidos, o la denegación de la práctica de pruebas contradictorias [642], o cualquier otra causa que permita cuestionar el resultado de la diligencia.

---

el art. 730 LECrim (LEG 1882, 16) , o a través de los interrogatorios, lo que posibilita que su contenido acceda al debate procesal público y se someta a confrontación con las demás declaraciones de quienes sí intervinieron en el juicio oral–». Se hace necesario invocar aquí a los efectos de dejar constancia de que no estamos ante simples requisitos sino de verdaderos aspectos a respetar el contenido de la STS. 814/2006 de 14 julio. Ponente: D. Joaquín Delgado García. En ella se analiza una prueba preconstituida consistente en unas grabaciones practicadas en la instrucción, y aunque válidamente incorporadas al proceso, finalmente en la vista oral no fueron objeto de escucha efectiva, sino que simplemente las partes acudieron al tradicional sistema de tenerlas por reproducida. Esto significó finalmente que el TS no la considerase como una prueba preconstituida, porque no se introdujo en el debate del juicio oral mediante su lectura, cosa que no se hizo. El Tribunal la consideró sólo como una mera diligencia sin darle el valor de prueba preconstituida.

[640] Vid. GIMENO SENDRA, Vicente. *Derecho procesal penal, segunda edición*. Op. Cit. Págs. 448 y 465. En las páginas mencionadas se alude a las vías de contradicción en las pruebas preconstituídas y anticipadas.

[641] Vid. GUDIN RODRÍGUEZ-MAGARIÑOS, Antonio Evaristo. «La protección de datos en el tratamiento procesal de los dispositivos de almacenamiento masivo de información». *La Ley Penal*, Nº 125, Marzo-Abril 2017, La Ley 3870/2017. Pág. 26. El autor expone de una manera muy acertada lo que constituye la práctica forense cotidiana, conforme a la cual en no pocas veces se utilizan sistemas de proyección en pantallas del contenido de la información que arroja el examen de determinados objetos de pericia como fórmula que sustituye a la necesaria lectura del contenido de los informes periciales como ordena la LEcrim en el art. 730. No obstante, señala acertadamente el hecho de que cuando el informe pericial es realizado por algún organismo oficial, no es necesaria la comparecencia en la vista oral de los redactores del informe, y ello por cuanto el art. 788.2 así lo contempla. Es cierto que el precepto lo dice, pero circunscrito a los informes periciales que versen sobre drogas tóxicas, como puede entenderse el contenido del Acuerdo del Pleno de la Sala segunda del Tribunal Supremo de 25 de mayo de 2005, y de la que nos sirve a título ejemplificativo de su aplicación la STS 901/2006 de 27 de septiembre. Ponente: Don Juan Ramón Berdugo Gómez de la Torre. Nada se dice en el precepto que se invoca sobre informes periciales realizados por organismos públicos cuyo objeto de pericia sea el relativo a datos informáticos. Me inclino a que en este caso, a diferencia de lo sostenido por el autor el contenido de la pericia sí que debe ser leído y explicado por parte de sus redactores, pues la finalidad del informe es hacer accesible a las partes, pero sobre todo al Tribunal el sentido de las conclusiones analizadas, y especialmente en este tipo de casos, si los datos informáticos permiten concluir con que alguno de los encontrados guardan relación con el hecho investigado, asimismo se hará más necesario si cabe la posibilidad de conocer de primera mano el contenido del informe si existen otras pericias contradictorias aportadas por las partes, y en tercer lugar habremos de asumir que no serán tan frecuentes tales pericial, como desgraciadamente resultan en los casos también muy masivos de los delitos contra la salud pública.

[642] Además, es muy posible que se recabe auxilio o cooperación judicial para la efectiva ejecución de dichas pruebas, incluso cuando son solicitadas por la defensa, lo que permite pronosticar un mayor incremento de estas peticiones en el futuro de lo que en la actualidad se hace. En apoyo de esta idea citaremos un párrafo de la STS 160/2016 de 1 de marzo, Ponente: Don Manuel Marchena Gómez. La citada resolución al amparo de la valoración jurídica relacionada con la pertinencia de la denegación de una prueba pericial informática interesada por una de las partes y que fue denegada, razona lo siguiente*: «Las razones de la pertinencia de un dictamen pericial como el que fue solicitado por la defensa y rechazado por el Tribunal a quo, se refuerzan a la vista de la ausencia de una petición judicial dirigida a las entidades Google España y Vimeo que habría permitido investigar con mayor rigor el rastro telemático del intruso.*

En definitiva, no se trata de restar valor probatorio a una prueba pericial informática por el simple hecho de que haya sido aportada por la acusación particular. Sobre todo cuando, como expresa la sentencia recurrida, la defensa tuvo cumplida oportunidad en el plenario de someter a contradicción los extremos del dictamen. Sin embargo, sea ese dictamen de carácter oficial o tenga su origen en expertos informáticos no adscritos a un centro de esa naturaleza, lo

El modo en que habitualmente se incorporarán al proceso los datos obtenidos mediante la práctica de esta diligencia será aportando los datos directamente obtenidos por la diligencia en el soporte en que estos consten, y junto a ellos, se aportará un informe pericial que analice y estudie el contenido de esos datos que fueron encontrados en el dispositivo físico o virtual[643], y los conecte con los hechos objeto de investigación. Esta forma es la más normal, sin que quepa descartar, en hipótesis otros medios como el reconocimiento judicial acerca de algún aspecto muy determinado[644].

De lo anterior puede concluirse con que el resultado de esta diligencia será subsumible en la categoría de la denominada prueba electrónica que contemplan, sin demasiada profundidad, las normas procesales penales[645].

La llamada prueba electrónica se define como *«aquella en la que intervienen las nuevas tecnologías en su formación y en su producción. Es decir, la tecnología puede afectar a la realidad que constituye la fuente de prueba, como al instrumento o medio a través del cual esa realidad pasa a ser reconocida por el juez o tribunal»*[646]. Este tipo de prueba ha dado lugar a que los autores se planteen su catalogación, bien como prueba de naturaleza documental, o bien otro tipo de prueba, en la medida en que el ámbito del proceso civil rige un modo de valoración diferente para las pruebas documentales y para las demás pruebas.

En este sentido, y partiendo de la distinción doctrinal entre fuentes de prueba y medios de prueba, puede señalarse que la fuente de prueba en el caso de las diligencias de investigación de los arts. 588 sexies, y 588 septies de la LECrim, vienen constituida por los datos que se encuentran en el dispositivo electrónico cuyo examen se haya ordenado judicialmente, y que pueden ser desde un pen drive encontrado, hasta el ordenador al que se accede o el repositorio en el que se encuentran

---

cierto es que la autoría de una intromisión en los sistemas informáticos ajenos exigirá, en buena parte de los casos, algo más que el conocimiento de una dirección IP y un nickname de usuario. Si a ello se añade que el desconocimiento de los términos del acceso al correo corporativo y al programa de edición de vídeos estuvo originado por no haber sido cursada la correspondiente solicitud judicial, los argumentos que respaldan la reivindicación de la defensa adquieren pleno significado». Como puede verse se extrae como idea esencial, además de la importancia debida a dicha prueba, un extremo hasta ahora no tenido en cuenta, y es el derivado de la investigación de oficio que corresponde al Juez instructor, de la cual se deduce en este tipo de casos la necesidad de intervenir en los supuestos en los que pudiera necesitarse dicho auxilio.

[643] Vid. DELGADO MARTÍN, Joaquin. «La prueba digital. Concepto, clases, aportación al proceso y valoración (1)» *Diario La Ley*, Nº 6, 11 de Abril de 2017. LA LEY 3841/2017 I. Pág. 1.

[644] Vid. DELGADO MARTÍN, Joaquin. «La prueba digital. ….. ». Op. Cit. Pág. 3. El autor considera que cualquier medio de prueba realmente sirve para poder incorporar datos electrónicos al proceso, sin embargo, la mayor parte de los casos serán los tres sistemas enumerados: documental, pericial e inspección ocular realizada por el Juez, el método más empleado para traerlos al proceso.

[645] Cfr. DELGADO MARTÍN, Joaquin. «La prueba digital. ….. ». Op. Cit. Pág. 1, que hace referencia a esta prueba aludida en el art. 299.2. LEC, a cuyo tenor: *"«También se admitirán, conforme a lo dispuesto en esta Ley, los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso».*

[646] Cfr. COLOMER HERNÁNDEZ, Ignacio, «La prueba tecnológica», en GONZÁLEZ CANO, María Isabel (Dir), *La Prueba. Tomo I. La Prueba en el Proceso civil*. Tirant lo Blanch. Valencia. 2017. Pág. 581

alojados los datos. Mientras, el medio de prueba viene constituido por el soporte en el que tales datos se aportan a las actuaciones y por el informe pericial en el que se interpreta y analiza la información que se hace llegar al Juzgado.

Las fuentes de prueba en general pueden ser muy variadas, porque en ellas es donde residen los aspectos que se deben llevar al procedimiento para que quede constancia de los diversos elementos que se están investigando, por eso, en realidad casi cualquier cosa llega a ser una fuente de prueba. La fuente de prueba en el caso de las diligencias de investigación electrónica, lo será el dato que se contiene en el dispositivo electrónico de cualquiera naturaleza y en el ordenador, en la medida en que son los que guardan los datos que a su vez tienen relación con el hecho penal investigado. Sin embargo, lo jurídicamente esencial es que la aportación e incorporación de esas fuentes al proceso, se haga aplicando las normas procesales que regulan los medios de prueba: por ejemplo, mediante el respeto a las normas que regulan la aportación de la prueba documental, o la prueba pericial, la testifical, o cualquier otra. Es por eso por lo que la doctrina mantiene que mientras las fuentes de prueba son muy amplias, los medios de prueba deben ser los previstos en las normas procesales, y en consecuencia el resultado de su práctica se puede incorporar al proceso, siguiendo las exigencias previstas para su práctica y desarrollo conforme a lo establecido en la ley procesal[647].

En lo que se refiere a la concreta incorporación al proceso de los datos obtenidos en las diligencias de investigación electrónica ordenadas judicialmente, no todas ellas cuentan con una regulación específica sobre las exigencias y requisitos que deben cumplir para la válida unión a las actuaciones del resultado probatorio obtenido. En este sentido, es preciso destacar el contraste que se da entre las diversas Secciones dentro del Capítulo V en relación con esta materia. Pues, respecto a la incorporación de datos de tráfico y asociados hay normas expresas, que no se olvide son de exclusiva aplicación a la intervención de comunicaciones electrónicas o telemáticas, que admiten la exclusión de aquellos contenidos de escaso o nulo interés o de los que afecten directamente a la vida privada de los interlocutores, por el contrario, la incorporación al proceso del análisis de los datos obtenidos mediante las diligencias de registro de datos electrónicos no está regulada específicamente en la LECrim, previendo exclusivamente que sea el auto en que se acuerde la

[647] Cfr. SANCHÍS CRESPO. Op. Cit. Pág. 71. De hecho la autora pone varios ejemplos muy significativos para distinguir la categoría, manifestando que por ejemplo en el caso de un documento, éste se considera como la fuente, y el medio de prueba es respetar «*la actividad procesal necesaria para incorporarla al proceso*», o en el caso de la testifical, el testigo es la fuente de prueba, y el medio es la correcta realización de su testimonio en el proceso, o en el caso de la pericial, la fuente es la cosa que será estudiada y el medio es la realización de la pericial conforme a las normas procesales: designación de perito, realización del informe, incorporación al proceso, etc.

práctica de la diligencia de registro de datos electrónicos el que concrete el modo de aportación al proceso de la información[648].

En este sentido, hay que tener en cuenta que, si bien es cierto que el juez instructor no está obligado a seguir las vías de incorporación del resultado de la práctica de las diligencias a las actuaciones que están previstas para las diligencias de interceptación de las comunicaciones, nada le impide seguir ese sistema, en aras a otorgar mayor seguridad jurídica al proceso de incorporación y evitar de este modo cualquier tipo de comportamiento arbitrario. De hecho, seguir estas premisas legales favorecería una mayor protección de los derechos del art. 18 CE, que es la finalidad perseguida por la ley.

Por su parte, no se puede olvidar que, sobre esta misma materia, en la LECrim hay algunas directrices a seguir para la inclusión en las actuaciones penales de los datos obtenidos en un registro electrónico[649]. Así, el art. 588 bis c LECrim prevé que en el auto, que acuerde el registro de datos, se fije la extensión de la medida, su finalidad, su alcance, la forma y la periodicidad en que deberá darse cuenta al juez instructor de su realización. Esta previsión se concreta en la diligencia de acceso a dispositivos de almacenamiento masivo en exigir que el juez de instrucción en el auto que acuerde la medida, se pronuncie sobre los términos y el alcance del registro, la posibilidad de realizar copias de los datos, de modo que quede garantizada su preservación[650] e integridad[651] para

[648] Esta es la opinión que parece desprenderse del autor Vid. GUDÍN RODRÍGUEZ-MAGARIÑOS, «La protección de datos en el tratamiento procesal de los dispositivos de almacenamiento masivo de información». Op. Cit. Pág. 28. Como puede deducirse de la lectura de su trabajo, este autor concluye que el auto que ordena la práctica de la diligencia es el que determinará la información que se está buscando, la que puede resultar relevante y la que, en suma deba finalmente incluirse en el procedimiento, si bien para ello el autor defiende la audiencia de todas las partes.

[649] STS 661/2017 de 10 de octubre. Ponente: Don Alberto Jorge Barreiro. Esta sentencia no profundiza desde una óptica más jurídica en cuáles deben ser los criterios que sirven para incorporar los datos que se han obtenido como fuente de prueba al proceso, pero, de su contenido se pueden deducir determinadas instrucciones. Por ejemplo, en el auto de entrada y registro en domicilio, puede incluirse, cuando la necesidad del supuesto lo requiere, no ya sólo la autorización para la entrada y registro en domicilio, sino también la incautación de información electrónica, e inclusive su volcado en el acto, apreciándose que ya se empiezan a dar algunos de los mecanismos que se apuntan en este trabajo como la presencia del LAJ. Se detecta que buena parte de los motivos de impugnación podrán ir por la vía de cuestionar el respeto y la garantía debida de la cadena de custodia. Se indica en la sentencia que: «*Por consiguiente, resulta incuestionable que concurrían sospechas muy fundadas y buenas razones para acordar la diligencia de entrada y registro, y así se plasmó en la autorización judicial concedida a través del referido auto. En el que no sólo se recoge la fundamentación indiciaria de la decisión adoptada, sino que se concreta en el fundamento jurídico primero la aplicación del art. 588 sexies de la LECr . y la procedencia de que se autorice la ocupación y posterior registro de los dispositivos almacenadores de memoria informática y cualesquiera otros vinculados a soportes de esa naturaleza. Se autorizaba además su posible volcado y clonado incluso in situ en el momento de hacer el registro a presencia del Letrado de la Administración de Justicia y del investigado, dada la urgencia de su realización en el caso de que les llevara a obtener información de otras actividades vinculadas con la actividad delictiva y personas investigadas, atendiendo a la gravedad del delito que se está investigando (actos de terrorismo islámico)»*

[650] Dicha preservación podría conseguirse por ejemplo mediante un sistema consistente en el volcado de los datos obtenidos o bien mediante la inclusión en las actuaciones del propio dispositivo incautado. No obstante, por algún autor se defiende la necesidad de homologar un proceso de aportación de la información electrónica a las actuaciones de suerte que pueda ser transparente y susceptible de ser comprendido el contenido que arroje la práctica de la diligencia realizada. (Vid. DELGADO MARTÍN, Joaquin. «La prueba digital. ….. ». Op. Cit. Págs. 4 y 9).

[651] Cfr. VALVERDE MEGÍAS, Roberto. Intervención de comunicaciones telemáticas y registro remoto. Op. Cit. Págs. 35 y siguientes. Ponencia realizada en los cursos de formación continuada realizados en fecha 27 de abril de 2016 bajo

poder, en su caso, realizar una prueba pericial que sirva al tribunal tanto para entender el contenido de los datos encontrados en el dispositivo, como igualmente para despejar cualquier duda de fidelidad en la prueba, o que la misma pueda ser sujeta a la posibilidad de contradicción a la que el investigado tiene derecho[652].

En lo que se refiere a la diligencia de acceso remoto a equipos la Ley también exige al auto judicial que determine su alcance, su modo de acceso, la aprehensión de los datos, cuáles serán los archivos relevantes para la causa, e incluso el programa que sirve para la ejecución de la medida, la realización de copias y las medidas de preservación (art. 588 septies a, apartado 2 LECrim). En este caso no se habla de prueba pericial, pero salvo este medio de prueba no hay otro más acertado para comprender el contenido de los datos.

En suma, en los dos casos puede decirse que la Ley sólo fija algunas pautas sobre la concreta forma de llevar a cabo las diligencias de investigación acordadas en el seno de las actuaciones, correspondiendo al juez en cada caso concreto la especificación de los pormenores de la práctica de las medidas para garantizar todos los derechos en juego y la utilizabilidad de la información obtenida en el juicio oral.

Además, no puede perderse de vista que la admisión y la práctica de estas diligencias debe guiarse por los criterios que la doctrina siempre ha considerado necesarios para esto: pertinencia, necesidad, licitud, y respeto de las normas procesales[653].

---

la denominación de *La interceptación de las comunicaciones telefónicas y telemáticas*. Pág. 29 y siguientes. Puede encontrarse el texto íntegro en el enlace de la página de Ministerio Fiscal: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20Valverde%20Meg%C3%ADas,%20Roberto.pdf?idFile=c740b0e1-8842-4ef7-8983-23c4a0732291
El autor se detiene específicamente en la necesidad de aportar la integridad de los datos obtenidos en el registro para que las partes puedan realizar un seguimiento total y pleno de la información obtenida. Igualmente defiende la mayor transparencia posible en el resultado en tanto que no existe durante ese proceso la concurrencia de Letrado de la Administración de Justicia, para lo cual demanda el uso de la firma digital oportuna, así como también certificación del sistema empleado para la extracción y lectura de los datos obtenidos. Sobre el segundo de los puntos mencionados considero necesario aportar la consideración textual que realiza el autor, que indica *«La primera pasaría por que los programas utilizados para los registros remotos sean analizados por un organismo público con competencia para la certificación de sistemas y programas, de tal manera que el certificado exponga las limitaciones y funcionalidades del programa sin necesidad de proporcionar el mismo a las defensas. La segunda consiste simplemente en proporcionar el programa a las defensas: teniendo en cuenta que, como se ha expuesto, la utilización de una herramienta informática de este tipo pasa por una fase de especialización y adecuación al sujeto concreto que se quiere investigar, el nivel de personalización puede llegar a ser tal que en cualquier caso no pueda ser utilizado en futuras investigaciones, en que habrá que enfrentarse otros equipos, otros sistemas operativos, otros programas,… o los mismos pero con las vulnerabilidades parcheadas por alguna actualización».*

[652] El art. 588 sexies c, párrafo 1 LECrim contempla, entre otras cosas, la posibilidad de que el auto establezca el modo en el que los datos encontrados en el dispositivo sean preservados a los efectos de que cualquiera de las partes pueda pedir, *«la práctica de un dictamen pericial»*.

[653] Cfr. DELGADO MARTÍN, Joaquin. «La prueba digital. ….. ». Op. Cit. Pág. 3. El autor hace una distinción de cada una de las fases y criterios por los que debe pasar la prueba electrónica para incorporarse al proceso. Concretamente reseña que bajo estos tres criterios debe entenderse lo que sigue: «*La prueba digital ha de ser relevante para acreditar los hechos objeto del proceso (thema decidendi), es decir, ha de existir una relación lógica entre el hecho que pretende acreditarse mediante el concreto medio probatorio y los hechos que constituyen el objeto de la controversia, así como*

En conclusión, la incorporación al proceso de la información obtenida después de realizar el registro de datos dependerá del modo en que el juez lo haya ordenado. El respeto a lo establecido por el juez es determinante para su válida inclusión en las actuaciones. De forma que lo habitual será que la incorporación de la información se realice mediante la aportación de los datos obtenidos, y de un informe pericial informático[654], que también se incorpora a las actuaciones, redactado por parte de los agentes encargados de la investigación, en el que se describan cuáles son estos datos, cuál es su contenido y en el que se ponga la información obtenida en relación con el objeto penal investigado. Una vez que se aporta, lo más habitual es que mediante providencia se una su contenido a las actuaciones, de lo que se dará traslado a las acusaciones y las defensas, para que éstas puedan impugnar su resultado, en orden a que sea expulsado el contenido de la diligencia de investigación del contenido final de las actuaciones[655], lo completen o lo impugnen mediante la aportación a su vez de otros informes complementarios.

6.2. La impugnación del resultado las diligencias de investigación.

El derecho a los recursos contra las resoluciones judiciales es parte del derecho a la tutela judicial efectiva[656]. El empleo de los recursos previstos en la ley, aplicados contra las resoluciones dictadas

---

una aptitud o idoneidad para formar la debida convicción del juzgador (pertinencia); Y ha de resultar útil para esclarecer los hechos controvertidos, esto es, su práctica ha de ser imprescindible o indispensable por no haber suficientes elementos probatorios que generen el convencimiento del juez acerca de lo que pretende probarse (necesidad). Téngase en cuenta que mientras el concepto de pertinencia despliega sus efectos de la fase de admisión de la prueba, el de necesidad actúa en el momento de su práctica.— En segundo término, la licitud, es decir, el respeto a los derechos fundamentales durante la práctica del concreto medio probatorio. — En tercer lugar, el cumplimiento de los requisitos exigidos por las leyes procesales (18) , es decir, que la prueba acceda al proceso de conformidad con los requisitos exigidos por la normativa procesal del correspondiente orden jurisdiccional (civil, penal, laboral o contencioso-administrativa)».

[654] Sobre pericial informática se puede consultar DELGADO MARTÍN, Joaquin. «La prueba digital. ….. » Op. Cit. pág. 3.

[656] STC 43/2000, de 14 de febrero. Ponente: Doña María Emilia Casas Bahamonde. En el fundamento jurídico tercero puede leerse con cita de otras sentencias del mismo órgano que: *«el acceso a la jurisdicción es un elemento esencial del contenido del referido derecho fundamental, el sistema de recursos frente a las diferentes resoluciones judiciales se incorpora al derecho a la tutela judicial efectiva en la concreta configuración que reciba en cada una de las Leyes de enjuiciamiento reguladoras de los diferentes órdenes jurisdiccionales, salvo en lo relativo a las Sentencias penales condenatorias (por todas, SSTC 37/1995, de 7 de febrero, fundamento jurídico 5.o; 211/1996, de 17 de diciembre, fundamento jurídico 2.o; 62/1997, de 7 de abril, fundamento jurídico 2.o; 162/1998, de 14 de julio, fundamento jurídico 3. ; 218/1998, de 16 de noviembre, fundamento jurídico 2.o, y 23/1999, de 8 de marzo, fundamento jurídico 2.o). De tal suerte que, en tanto el principio hermenéutico pro actione despliega su plena operatividad cuando del acceso a la jurisdicción se trata, en el ámbito del acceso a los recursos —y al margen de la ya referida singularidad que representa el proceso penal— el control constitucional de las decisiones judiciales que declaran la inadmisibilidad del recurso ha de ceñirse a los cánones del error patente, la arbitrariedad o la manifiesta irrazonabilidad (de entre las más recientes, SSTC 162/1998, de 14 de julio, fundamento jurídico 3.o; 168/1998, de 21 de julio, fundamento jurídico 4.o; 192/1998, de 29 de septiembre, fundamento jurídico 2.o; 216/1998, de 16 de noviembre, fundamento jurídico 2.o; 218/1998, de 16 de noviembre, fundamento jurídico 2.o; 236/1998, de 14 de diciembre, fundamento jurídico 2.o, y 23/1999, de 8 de marzo, fundamento jurídico 2.o)» (fundamento jurídico 4.o)».*

en el proceso penal configuran la principal actuación de las defensas y de las acusaciones para combatir el resultado de las diligencias de investigación electrónica unidas al proceso. La tipología y el número de estos recursos están tasados, y son uno de los principales medios con los que cuentan las partes para incidir en la práctica de las diligencias de investigación o en su resultado.

Uno de los aspectos más importantes cuando se quiere recurrir este tipo de diligencias es adecuar el momento temporal apto para recurrir. Y es que, la impugnación de una diligencia de investigación, debe contemplar una circunstancia, que no se da en el resto de actos procesales, que se concreta en la apertura de una pieza separada y secreta. De manera que esta circunstancia conlleva que la defensa ignore el contenido o el resultado de la diligencia, y se le prive en esos instantes de analizar la legalidad de la medida, y no pueda comprobar su ajuste a los requisitos y exigencias propias de cada una de ellas. Por lo tanto, sólo se abre la vía de recurso cuando dicha pieza queda despojada de su carácter secreto y le sea notificada.

En este sentido se debe considerar que el *dies a quo* para el inicio del cómputo del plazo para su interposición, es el siguiente al de su notificación. Por ello, con carácter general, tras la notificación del auto que ordene una diligencia de investigación es cuando cabrá interponer el recurso que proceda según lo previsto en la LECrim. Por el contrario, cuando la pieza hubiera estado declarada secreta, el plazo para recurrir se iniciará una vez alzado el secreto, y notificado su contenido a las partes.

La resolución judicial relativa a la práctica de una diligencia puede recurrirse ante el mismo órgano que la acordó o ante el superior. La finalidad que se busca en el primer caso es una reconsideración de la decisión adoptada porque exista algún error o se haya producido una vulneración de alguna garantía durante su adopción o práctica. En el segundo supuesto, el derecho a los recursos ante instancias judiciales superiores, busca un reexamen de la resolución recurrida, que termine con su confirmación o revocación. En todo caso el recurso debe ser planteado en el primer momento en que se pueda hacer, porque, aunque suele ser habitual dejar las impugnaciones para momentos en los que el proceso ya está muy avanzado, suele ser una táctica que da pocos frutos, al exigirse jurisprudencialmente una denuncia inmediata ante cualquier defecto procesal que se intenta denunciar por la vía de los recursos.

Los modos de impugnación de resoluciones judiciales penales previstos en nuestro ordenamiento se disponen en el artículo 216 LECrim, que establece que, contra las decisiones del Juez de Instrucción, en general cabe interponer los recursos de reforma, de apelación y de queja.

6.2.1. Recurso de reforma.

El recurso de reforma se define doctrinalmente como *«un medio de impugnación ordinario, no devolutivo, ni, con carácter general suspensivo, que procede contra las resoluciones interlocutorias dictadas por un órgano unipersonal y cuya interposición constituye, en determinados supuestos, presupuesto de admisibilidad de otros recursos»*[657].

Con la interposición de este recurso se persigue cambiar el contenido de la resolución judicial adoptada, en todo o en parte. Se pretende del Juez de Instrucción, que ha adoptado la concreta medida de investigación que la deje sin efecto, o bien la modifique alguna parte de la misma[658].

La concreta impugnación del registro de datos acordado ha de hacerse tras su práctica efectiva, y una vez acordado el levantamiento del secreto de la pieza, porque sólo así se puede conocer en detalle el contenido de las resoluciones que habilitaron su ejecución. Los recursos en estas situaciones suelen dirigirse a aspectos como una hipotética forma indebida de llevarlo a cabo, la vulneración de algún requisito procesal, etc.

Es el tipo de recurso más inmediato, el primero en la escala de los existentes. Por eso resulta un medio apto para denunciar ante el juez de instrucción cualquier posible vulneración de derechos y garantías procesales cometidos al practicar la diligencia que pudiera originar la nulidad de actuaciones. Con esta forma de proceder de la parte defensora se evita la posibilidad de que se le pueda imputar que con su conducta no haya cumplido con el deber de denuncia de los vicios procesales en los que se haya podido incurrir en la adopción y práctica de la diligencia[659].

Lo más aconsejable, y más respetuoso con los derechos del investigado es advertir en la primera oportunidad que se tenga de un hecho con trascendencia anulatoria, antes de que pueda esgrimirse que pudo haberse advertido antes y no se hizo, lo que ratifica la corriente doctrinal mayoritaria, que es proclive a esto, con el fin de permitir a los causantes de la hipotética indefensión alegada como

---

[657] Cfr. GIMENO SENDRA, Vicente. *Derecho procesal penal*, Segunda Edición. Op. Cit. Pág. 872.

[658] En este sentido, la parte puede pretender con el recurso de reforma que se modifique el modo en que debe ejecutarse la diligencia, solicitando que se practique de un modo distinto al decretado, o que se reforme o complete una parte del mismo.

[659] La cuestión sobre el momento adecuado para poner de manifiesto la posible vulneración de derechos fundamentales es un aspecto que la propia doctrina no tiene claro; puede consultarse al respecto NAVARRO MASSIP, Jorge, «El maquiavelismo probatorio de la prueba ilícitamente obtenida en el proceso penal», en *La prueba en el proceso penal,* Thomsom Reuters Aranzadi, Pamplona, 2016. Pág. 45. El autor en este caso lleva al Juicio oral la vulneración del posible derecho fundamental aplicable, si bien termina acogiendo la vía seguida por otros autores, y viene a establecer que lo conveniente es efectuar la denuncia de la posible vulneración del derecho afectado lo antes posible (página 46). Por su parte en PAZ RUBIO, José María, MENDOZA MUÑOZ, Julio, OLLE SESÉ, Manuel y RODRÍGUEZ MORICHE, Rosa María, *La prueba en el proceso penal. Su práctica ante los Tribunales*. Colex, Madrid, 1999 (págs. 409 a 412), también se venía poniendo de manifiesto esta absoluta falta de claridad en lo relativo al momento de la impugnación de la prueba ilícita. Se señala en la última obra citada la limitación en la fase de instrucción para depurar la posible nulidad, si bien no la cierra porque el Juez instructor también está obligado por el contenido del art. 11.1 LOPJ. Alude como única vía de recurso de la decisión vulneradora de derechos fundamentales las relativas a la sentencia de fondo.

motivo de recurso, que puedan repararla. Así se evita que sea un tribunal superior el que deba enmendar este extremo, pese a que el vicio anulatorio no se hubiera alegado con anterioridad [660]. De hecho, para poder acudir al recurso de amparo es necesario haber agotado previamente la vía judicial en la que dicha vulneración se produjo. En caso de que no se haga, no se puede alegar la vulneración del derecho de defensa, porque no se ha permitido al tribunal, que ocasionó la presunta vulneración, la posibilidad de poderla enmendarla[661].

La resolución judicial, motivada y fundada en derecho[662] tendrá que ser la que valore, previo informe del Ministerio Fiscal, en el que se adhiera o se impugne dicho recurso, las cuestiones

---

[660] Vid. MIRANDA ESTRAMPES, Manuel. *El concepto de prueba ilícita y su tratamiento en el proceso penal*. BOSCH. Barcelona. 2005. Capítulo III en su integridad.

[661] Citaré en este caso, por reciente, una SAP de Madrid, secc, 16, 32/2018, de 16 de enero. Ponente: Don Alberto Molinari López Recuero. La citada sentencia, haciendo acopio de numerosas resoluciones del TC viene a recordar que: «*La ausencia de contradicción y defensa de alguna de las partes en el proceso que resulta de su actuación negligente no puede encontrar protección en el art. 24.1 CE ; así ocurre cuando la parte que pudo defender sus derechos e intereses legítimos a través de los medios que el ordenamiento jurídico le ofrece no usó de ellos con la pericia técnica suficiente, o cuando la parte que invoca la indefensión coopere con la conducta a su producción, ya que la indefensión derivada de la inactividad o falta de diligencia exigible al lesionado, o causada por la voluntaria actuación desacertada, equivoca o errónea de dicha parte, resulta absolutamente irrelevante a los efectos constitucionales, porque el derecho a la tutela judicial efectiva no impone a los órganos judiciales la obligación de subsanar la deficiencia en que haya podido incurrir el planteamiento defensivo de la parte (STC 167/88 , 101/89 , 50/91 , 64/92 , 91/94 , 280/94 , 11/95)"*.....para seguir algún párrafo más adelante indicando que: *"es también unánime la precisión jurisprudencial que se refiere al comportamiento procesal del recurrente a lo largo del procedimiento y en sus diversas fases, pues tal constatación es determinante para la aplicación de la buena o mala fe procesal y, sobre todo, para valorar en toda su intensidad la real presencia de una situación de indefensión que anule de manera efectiva las posibilidades de defensa o haya impedido la rectificación de comportamientos procedímentales irregulares en momentos especialmente previstos para su denuncia y corrección con merma mínima de otros derechos de igual rango como pudiera ser, entre otros, el derecho a un proceso sin dilaciones indebidas. De ahí que, en pura correspondencia con al proscripción constitucional garantista de un proceso justo, se plasman exigencias en evitación de abusos o de actividades interesadas en la confirmación artificial de situaciones de indefensión que, al alcanzar cotas de imposible corrección, hagan precisa una técnica quirúrgica anulatoria nunca deseable, aunque si perseguida, por quienes, sometidos a un proceso incriminatorio con reales posibilidades de condena, consiguen así dilatar al máximo la conclusión del mismo».*

[662] ST AP de Guadalajara 24/2017, de 17 de enero. Ponente Dña. María Victoria Hernández Hernández. Esta resolución, con cita de muchas resoluciones del TC, viene a sostener este aspecto como esencial indicando que: «*Para finalizar no puede obviarse que el deber de motivación de las resoluciones judiciales viene exigido por el derecho a la tutela judicial efectiva (art. 24 CE), porque como señalan la STC 169/2002, de 30 de septiembre (RTC 2002, 169) (FJ 2) y STC 114/2003 de 16 junio (RTC 2003, 114) , la falta de motivación provoca una denegación de justicia, el órgano judicial no tutela los derechos o intereses legítimos sometidos a su jurisdicción. Como recuerda la TC de 17.2.1998 (RTC 1998, 36) , la motivación es "una garantía del justiciable mediante la cual, sin perjuicio de la libertad del Juez en la interpretación de las normas y los hechos, se puede comprobar que la solución dada al caso es consecuencia de una exégesis racional del ordenamiento y no el fruto de la arbitrariedad"; deber de motivación, como expresa el Auto del TS, Sala 2ª de 6.11.2014 (JUR 2015, 22238) que aun cuando "no alcanza a la contestación pormenorizada de todos y cada uno de los argumentos utilizados como apoyo de la pretensión" si exige "una respuesta que deje de manifiesto que la resolución no es arbitraria, sino fundada en razones que tienen su apoyo en el Derecho vigente. Es decir, que la resolución dictada contenga la fundamentación suficiente y necesaria para que los litigantes conozcan las razones que condujeron a su adopción y les permita, así, configurar un recurso contra ella».*

En el mismo sentido la STC nº 57/2007 de 12-3-2007 (RTC 2007, 57) expresa que «La exigencia de motivación de las Sentencias "está directamente relacionada con los principios de un Estado de Derecho (art. 1.1 CE) y con el carácter vinculante que para Jueces y Magistrados tiene la Ley, a cuyo imperio están sometidos en el ejercicio de su potestad jurisdiccional (art. 117 CE , párrafos 1 y 3; SSTC 24/1990, de 15 de febrero (RTC 1990, 24) , FJ 4 ; 35/2002, de 11 de febrero (RTC 2002, 35) , FJ 3). Por ello, hemos dicho que la existencia de una motivación adecuada y suficiente, en función de las cuestiones que se susciten en cada caso concreto, constituye una garantía esencial para el justiciable, ya que la exteriorización de los rasgos más esenciales del razonamiento que han llevado a los órganos judiciales a adoptar su decisión -haciendo explícito que ésta corresponde a una determinada

introducidas por la parte en su recurso, es decir, si concurren los defectos apreciados, despejando al mismo tiempo, la posibilidad de quien denuncia tales circunstancias a las instancias superiores, conforme a los recursos específicos.

6.2.2. Recurso de Apelación.

El segundo escalón en la pirámide legal de los recursos es el recurso de apelación. No se trata de un recurso genérico, sino que sólo cabe interponerse cuando la legislación lo permita expresamente -ex art. 218 LECrim-.

La reforma operada en la regulación del recurso de apelación de dos mil quince, con la finalidad de *"mejora en la justicia penal"*, ha introducido la reclamada doble instancia penal en todos los ámbitos. De este modo se introduce la posibilidad de recurrir en apelación determinadas sentencias que antes estaban huérfanas de esta posibilidad[663].

Pero la apelación que aquí se trata no es la que se interpone como recurso contra una sentencia, sino el medio de impugnación que se despliega contra el auto acordando la práctica de una diligencia de investigación tecnológica en la fase de instrucción. Estas decisiones pueden impugnarse en esta fase procesal para que el tribunal superior aprecie la concurrencia de algún defecto que invalide la diligencia y su resultado.

Por otra parte, no debe perderse de vista que el valor probatorio del resultado de la diligencia de investigación realizada durante la instrucción puede ser discutido durante el juicio oral, y por ello si la evidencia obtenida con la diligencias es objeto de valoración en la sentencia dictada por el órgano enjuiciador, puede ser causa para entablar un eventual recurso de apelación interpuesto contra la sentencia que se dicte. Por tanto, si la valoración que hace la sentencia sobre la diligencia y su resultado conforma un aspecto determinante del fallo, contrario a los intereses del recurrente, que introdujo debidamente al inicio del juicio oral o incluso antes, aspectos como la validez de la

---

interpretación y aplicación de la ley-, permite apreciar su racionalidad, además de facilitar el control de la actividad jurisdiccional por los Tribunales superiores, y, consecuentemente, mejorar las posibilidades de defensa por parte de los ciudadanos de sus derechos mediante el empleo de los recursos que en cada supuesto litigioso procedan (STC 209/1993, de 28 de junio (RTC 1993, 209) , FJ 1) ...».

[663] Sobre la doble instancia penal puede consultarse en Vid. ARMENTA DEU, Teresa. «La reforma del recurso de Apelación y la generalización de la segunda instancia»". *JUSTICIA: Revista de Derecho procesal.* Num: 1/2016. enero de 2016. Págs. 43 a 95.

diligencia, o defectos en su practica en el juicio oral, la apelación se dirigirá a combatir este valor otorgado[664].

En estos casos que se han indicado, el recurso de apelación ya no estará analizando la diligencia de investigación como lo hacía durante la instrucción, sino que ahora se combatirá la diligencia debido a su valoración como prueba realizada por el juzgador, y que ha podido servir para fundar un pronunciamiento desfavorable al recurrente. Sin embargo, tampoco es descartable que en el recurso se puedan plantear pretensiones anulatorias en relación con los defectos procesales que se hayan podido cometer durante su práctica, pero, sin duda, el grueso de la impugnación descansará sobre su validez como prueba.

El art. 790.2 LECrim, que fija las causas o motivos de la apelación, incluye entre los mismos: la valoración errónea de la prueba; la eventual existencia de quebrantamiento de normas y garantías procesales, motivo en el que se verá amparada la mayor de las veces el cuestionamiento al que se somete alguna de las diligencias limitativas de los derechos del art. 18 CE; o cualquier otra infracción de normas del ordenamiento.

El empleo de este tipo de recurso, ajustándolo al caso que se trate, persigue básicamente lo mismo que en el caso del recurso de reforma, es decir, dejar sin efecto la resolución judicial que acordó la medida, o bien se busca mediante su estimación limitar el resultado obtenido mediante su práctica de alguna manera[665]. En el recurso de apelación se puede pretender la modificación de algún aspecto de la diligencia; que se realice de una manera distinta; que se acuerde la práctica misma de la diligencia, lo que normalmente será causa de interposición de recurso por las acusaciones[666], por no estar conformes con el método empleado para acceder a la información, bien por ser muy

[664] Además de esta vía, cabe cuestionar la validez de las diligencias en fase de enjuiciamiento dentro de las cuestiones previas que se plantean al inicio de las sesiones del juicio oral. Al respecto es preciso señalar que alguno de los Magistrados que conforman el Tribunal Supremo abogan por la posibilidad de que sea introducida en nuestro derecho procesal penal la posibilidad de llevar a cabo una suerte de vista previa al juicio oral en orden a poder determinar si determinadas diligencias de investigación que han sido tenidas en cuenta por el Juez Instructor pudieran haber provocado alguna clase de vulneración de derecho constitucional. Así puede comprobarse DEL MORAL GARCÍA, Antonio. *«¿Cuándo debe declarar la inutilizabilidad de un medio de prueba de vulneración de derechos fundamentales? -Reflexiones al hilo de la STS 106/2017-.». Revista electrónica El Derecho* Francis Lefebvre, correspondiente al 18-04-2017. Págs. 3 a 10. *Enlace:* http://www.elderecho.com/tribuna/penal/Inutilizabilidad-prueba-vulneracion-derechos-procedimiento-penal_11_1079305001.html

[665] SAP de Jaén 553/2017 de 3 de septiembre. Ponente: Doña María Fernanda García Pérez. En esta sentencia la AP se pronuncia sobre el acceso a determinados dispositivos, como lo eran en este supuesto determinados teléfonos móviles y se recurre en apelación la ausencia de motivación suficiente.

[666] En el Auto de la AP de Pontevedra (Sección 5ª) 794/2017 de 9 noviembre. Ponente: Dña. María Belén Rubido de la Torre, se estima parcialmente un recurso de apelación que interpone la acusación particular perdonada en la causa en la que se había solicitado el registro de un ordenador, en el sentido de ordenar al Juzgado instructor que se quedase con un ordenador como prueba de convicción y una vez efectuadas las declaraciones de los investigados se procediera en base al criterio judicial que fuese con respecto a esta diligencia de investigación.

estricto[667], o bien por ser muy amplio[668] el elegido o por el acto consistente en la incautación del dispositivo[669].

El recurso de apelación se podrá utilizar frente a las decisiones judiciales relativas las diligencias de registro de datos, bien sea por la vía de valoración de prueba, bien sea por la infracción de normas procesales. En cualquier caso, para poder alegar posteriormente la infracción de normas constitucionales, debió plantearse el recurso de reforma, o bien directamente el recurso de apelación.

El art. 790.2 LECrim exige haber hecho constar la existencia de la posible infracción, a los efectos de que la misma pudiera ser subsanada, pues de no haberse hecho, ello puede significar la inadmisión del recurso. Por tanto, no debe esperarse al recurso de apelación para alegar la vulneración, sino que se ha de permitir al órgano jurisdiccional que adoptó la medida o decisión que causa la vulneración de derechos fundamentales, que pueda enmendarla. Para ello desde que se aprecia tal posible vulneración de derechos debe hacerse saber al órgano que la causa para evitar

---

[667] Resulta muy interesante el contenido de la Auto de la AP de Barcelona 215/2017, de 1 de marzo. Ponente: Doña Elena Guindulaín Oliveras. Este auto entra a considerar qué método es más ajustado a la hora de realizar el volcado de datos contenidos en un dispositivo a la par que con ello se garantice también el derecho a la intimidad de las partes. La en su recurso de apelación solicitaba que la búsqueda de información contenida en los dispositivos se realizase mediante lo que se conoce como *"búsqueda ciega por palabra clave",* es decir, el empleo de un sistema que filtrase la información obtenida por parte de los buscadores de la información depositadas en esos dispositivos; por el contrario la fiscalía se opuso a ello en tanto que ello podría coartar las posibilidades de obtener información suficiente, por cuanto podría estar oculta bajo palabras, números o signos que no fueran los empleados como palabras clave. El Tribunal desestima la petición alegando que son dos cosas diferentes el modo de obtener la información y otra el empleo de la misma. Se dice que: *toda vez que el volcado de la información obrante en los ordenadores intervenidos y archivos informáticos de los investigados debe realizarse en su integridad, pues no existe precepto alguno en la LECRM, que limite a este instructor obtener de forma integra los datos de dichos archivos, tal como se regula en el artículo 588 bis y ss. de la LECRM. De tal suerte que el copiado y volcado de los archivos debe ser en su totalidad, mientras que la forma en que se extraigan los datos de cada archivo informático deberá atender al interés de la investigación, siguiendo diferentes criterios ajustados a aquellas y siempre con respeto a la esfera personal e intima de los investigados, como ya se explicita en el auto de entrada y registro de fecha 12 de julio de 2016. Pues en caso contrario podría darse el supuesto de limitar el alcance de la información que puede obtenerse en el volcado del material informático aprehendido o dar a conocer a las partes implicadas el contenido de lo instruido, conocimiento limitado al ser secretas las actuaciones.* En términos similares podemos destacar el contenido del auto de la AP de Murcia (sección 3ª) 939/2017 de 27 octubre. Ponente: Doña Ana María Martínez Blázquez.

[668] Auto de la AP de Tarragona 615/2017, de 24 de noviembre. Ponente: Don Francisco José Revuelta Muñoz. El mencionado auto estima parcialmente un recurso de apelación contra un auto que ordenaba el examen de determinados dispositivos. En este caso se avaló por el Tribunal la amplitud de la medida y la ausencia o falta de garantías suficientes con respecto a datos de terceros, que podían ver como se vulneraba su derecho a la intimidad. Dice el auto que: «*Tal y como refiere la parte apelante, la utilización de palabras de naturaleza discriminadora, la intervención de las partes en el volcado de la información...entre otras, habrían sido medidas que habrían garantizado más intensamente el derecho a la intimidad o a la reserva o confidencialidad de aquellos documentos ajenos a la causa».*

[669] Auto de la AP de Soria 167/2017, de 26 de septiembre. Ponente: Doña Belén Pérez-Flecha Díaz. En la resolución se resuelve un recurso de apelación que se interpone contra una resolución del Juzgado de Instrucción que denegaba la entrega de determinados artefactos ocupados en un registro. Finalmente el Tribunal estima parcialmente el recurso en la medida en que no todos los objetos presentan el mismo interés y relación con los hechos, pero sobre todo aplica el principio de motivación individualizada contenido en la nueva regulación de la diligencia de registro de dispositivos de almacenamiento masivo y concluye con que *«no todos los objetos incautados deben quedar bajo la custodia judicial, sino únicamente aquellos que tengan relación con el delito investigado o que hayan podido obtenerse con sus ganancias, y siempre bajo el principio de proporcionalidad».*

que un pronunciamiento posterior ponga de manifiesto que no se agotaron las instancias que pudieran haberlo resuelto[670].

6.2.3. Recurso de casación.

El recurso de casación es una figura fundamental, erigiéndose como la última vía de la estructura jurisdiccional para impugnar una decisión. Su regulación ha sido recientemente reformada, por parte de la Ley 13/2015.

Es un recurso «*extraordinario, devolutivo y suspensivo*»[671]. El conocimiento del Tribunal en la casación se limita a determinados aspectos legales y procesales[672], por lo que no se puede valorar nuevamente la prueba, y ha de limitarse a examinar si se ha aplicado correctamente la ley en sus aspectos sustantivos o procesales. También forma parte de su objeto analizar si la sentencia recurrida es contraria a la doctrina jurisprudencial asentada sobre un determinado particular que aborda[673], y también se permite que el Tribunal de casación aprecie vulneraciones de derechos fundamentales.

---

[670] La STC 188/1998 de 28 de septiembre. Ponente: Don Fernando García-Mon y González Regueral establece en su fundamento segundo que: *«[l]a pronta y formal invocación en el proceso ordinario del derecho fundamental que se estima vulnerado hace posible su inmediata e idónea reparación, por el órgano judicial a quien se reprocha la infracción; evita la reprobación constitucional de una actuación judicial sobre cuya irregularidad no había sido advertido su agente; estratifica racionalmente la jurisdicción de amparo y, con ello, posibilita la plena subsidiariedad y "la propia funcionalidad de la jurisdicción constitucional" (STC 168/1995); y, en fin, preserva el itinerario procesal posible de la cuestión que tiene por centro un derecho fundamental y, por ello, su completo debate y análisis por las partes implicadas en el proceso, por el órgano judicial directamente afectado, y por los demás órganos judiciales con jurisdicción en el mismo».*

[671] Cfr. MARTÍNEZ ARRIETA, Andrés. *El recurso de casación penal. Control de la presunción de inocencia.* Comares. Granada. 1996. Pág. 17.

[672] La STS 645/2017, de 2 de octubre. Ponente: Don Juan Ramón Bendigo Gómez de la Torre, pone el acento en la funci*ón propia de la casación como mecanismo que a su juicio consagra la doble instancia. Sobre este aspecto dice : «Así como primera reflexión en SSTS 41/2009 de 29.1 , 168/2009 de 12.2 , 717/2009 de 17.6 , 438/2012 de 16.5 , 838/2014 de 12.12 , 40/2015 de 12.2 , 467/2015 de 20.7 , 547/2015 de 6.10 , 497/2016 de 9.6 , 240/2017 de 5.4 , 492/2017 de 29.6 , hemos declarado que debemos recordar que en sus orígenes históricos, la casación no era sino un control de legalidad referido a la interpretación y aplicación de la ley por los Tribunales, a efectuar por el Tribunal de Casación que en funciones de verdadera "policía jurídica" depuraba y eliminaba aquellas resoluciones judiciales que se apartaban de la interpretación correcta fijada, precisamente, por la Sala de Casación, que de este modo se convertía en garante y custodio del principio de seguridad jurídica, esencial en todo sistema jurídico y al que se refiere el art. 9 apartado 3 de la Constitución en términos de existencia y de efectividad "....la Constitución garantiza.... la seguridad jurídica...." de ahí su naturaleza de recurso extraordinario. Con ello se garantizaba, igualmente el principio de igualdad ante la Ley, pues quedaba garantizada una idéntica interpretación y aplicación de la misma en todos los procesos.*

Es precisamente en referencia a los juicios del Tribunal del Jurado que esa nota brilla con luz propia en la medida que la casación descansa sobre el recurso de apelación , al contrario de lo que ocurría en los delitos competencia de las Audiencias articuladas sobre la instancia única y la casación, antes de la reforma operada por Lo. 41/2015 de 5.10».

[673] La STS 641/2017, de 28 de septiembre. Ponente: Don Juan Ramón Bendigo Gómez de la Torre, trata de una cuestión muy interesante, el alcance de la facultad revisora del Tribunal Supremo sobre la infracción de normas jurídicas. La sentencia versa sobre la posibilidad de que una determinada sentencia recurrido en casación, incluso con pronunciamiento absolutorio con respecto al acusado pueda ser objeto de revocación y transformarse en cambio en una

Los aspectos relativos a la adopción de cualquiera las dos diligencias de investigación desarrolladas en este trabajo pueden recurrirse en casación por infracción de ley del art. 849 LECrim. El apartado 2º de dicho artículo, permite interponer casación por este motivo en los casos en que *«haya existido error en la apreciación de la prueba, basado en documentos que obren en autos, que demuestren la equivocación del juzgador sin resultar contradichos por otros elementos».* Así, si en la sentencia de apelación se ha valorado el resultado de las diligencias de manera errónea, o se ha ignorado alguna prueba que las cuestione, es posible recurrir en casación.

En este supuesto no cabe aludir a la infracción de normas procesales, por lo que bajo este motivo no se puede cuestionar el modo en que la diligencia fue realizada al ser una cuestión procesal, vedado a la infracción de ley. Por tanto, el cuestionamiento de la sentencia ha de recaer en el modo en que la diligencia practicada fue valorada por el tribunal enjuiciador.

El recurso de en casación por quebrantamiento de forma también puede interponerse por cuestiones relacionadas con esta diligencia. Se exige para ello que concurra alguno de los supuestos del art. 850.1º LECrim[674]. Mediante esta vía se combate el resultado de la diligencia por vía indirecta, al haber sido denegada una diligencia contradictoria o alguna otra prueba cuya finalidad pueda ser desacreditar a esta. Para ello debe formularse la oportuna protesta cuando esto acontece, pues de no haber mostrado este comportamiento contrario a la decisión adoptada se desestimará el recurso.

Los argumentos que se suelen emplear, tanto en el recurso de casación, como en los anteriores pueden ser muy diversos[675], abarcando múltiples variables procesales y de derecho sustantivo. No obstante, la práctica diaria permite afirmar que uno de los motivos de recurso que más se esgrime a la hora de recurrir las resoluciones judiciales relativas a alguna de las diligencias de investigación

---

sentencia condenatoria. Al respecto, resultan de interés las propias palabras del TS cuando alude a la función propia de la casación, diciendo que : «*La función esencial de esta Sala Segunda del Tribunal Supremo, en la que actúa específicamente como el órgano superior, o más propiamente supremo, del orden jurisdiccional penal, conforme a la función que le atribuye el art. 123 CE , es la que realiza a través del cauce de la infracción de ley, corrigiendo errores de subsunción y fijando criterios interpretativos uniformes con la finalidad de garantizar la unidad del ordenamiento penal, y con ello los principios de seguridad jurídica, predictibilidad de las resoluciones judiciales e igualdad de los ciudadanos ante la ley, sin perjuicio de que, a través de los motivos por quebrantamiento de forma, unifique también el ordenamiento procesal penal".* Es decir se parte de la función correctora y creadora de pareceres, que la sala denomina *"función nomofiláctica y unificadora, sin restricciones impuestas, o auto restricciones injustificadas, tanto en los supuestos en los que los órganos sentenciadores interpretan erróneamente los tipos penales en perjuicio del reo como si lo hacen en perjuicio de las víctimas o perjudicados".* Además la sentencia realiza una breve consideración sobre varios de los motivos de casación, siendo algunos de ellos el relativo al error en la valoración probatoria, indicando la resolución sobre el particular la sentada doctrina conforme a la cual " *Se ha reiterado hasta la saciedad que el recurso de casación no es una apelación y que, por tanto, el debate sobre la valoración probatoria está más limitado".* También se alude al recurso de casación por *"infracción de Ley por haber concurrido error en la apreciación de la prueba en los términos prevenidos en el artículo 849.2 LECrim";* y también al motivo de casación basado "*en motivo de denegación de diligencia de prueba previsto en el artículo 850.1 LECrim».*

[674] La norma contempla el acceso como motivo de casación por quebrantamiento de forma *«cuando se haya denegado alguna diligencia de prueba que. propuesta en tiempo y forma por las partes, se considere pertinente».*

[675] Pueden citarse como resoluciones judiciales en las que se realiza alusión a la nulidad de actuaciones la STS 546/2017, de 12 de julio. Ponente: Don Luciano Varela Castro (relativa a la nulidad de actuaciones derivada de una falta de motivación)

que limitan derechos fundamentales es la nulidad en alguno de los aspectos que tienen que ver con su adopción. En todo caso, el que se emplee la nulidad como motivo de recurso, no descarta la posibilidad de que pueda emplearse el incidente de nulidad de actuaciones propiamente dicho[676] cuando concurran los casos para ello[677]. Además, el empleo de la nulidad como argumento sirve tanto para combatir el contenido de la resolución por la vía de los recursos oportunos previstos en la ley como para hacer valer nuevamente este argumento en las instancias superiores, en caso de que la petición de declaración de nulidad de la resolución no se estime, mientras que, por el contrario, si no se hace valer esto en la primera instancia, no podrá sostenerse en las sucesivas.

6.3. Valoración de la prueba obtenida mediante la práctica de las diligencias de acceso y registro electrónico. Determinaciones para la validez de la prueba de datos electrónicos.

El art. 283 de la LEC [678] fija tres criterios para la admisión de medios de prueba por parte del tribunal y su práctica por el mismo, fijando que las pruebas que se propongan han de ser pertinentes, útiles y lícitas[679]. De hecho, lo primero que el juez encargado de resolver el asunto debe hacer es pronunciarse sobre la admisión de las pruebas propuestas por las partes para que se practiquen en la vista.

---

[676] Vid. ÁLVAREZ SÁNCHEZ DE MOVELLÁN, Pedro. *El incidente de nulidad de actuaciones: solución o problema frente a la resolución firme.* Madrid. Dykinson. 2015. Pág. 90.

[677] Sirva como ejemplo de la necesidad de este aspecto lo contenido en la STS 508/2017, de 4 de julio. Ponente: Don Manuel Marchena Gómez. En ella se puede apreciar la necesidad de hacer denuncia previa bien por la vía de recurso o bien por la que se estime adecuada del extremo que cause alguna vulneración de derechos. En este caso la sentencia alude a la alegación efectuada por la defensa conforme a la cual se habría accedido al contenido de una cámara de fotos digital sin contar con autorización, y ello con la finalidad de identificar al titular. No se interpuso recurso alguno ni se instó nulidad previa. Este aspecto finalmente conlleva la desestimación del recurso de casación sobre ese aspecto. Dice la sentencia: «*Fue en la fase de conclusiones definitivas -como pone de manifiesto el soporte digital en el que fueron grabadas las sesiones, cuyo contenido ha sido examinado por la Sala- cuando la defensa instó como «cuestión previa» la nulidad de actuaciones. La propia presidenta del órgano de enjuiciamiento hizo ver a la Letrada que asumió en juicio la defensa del recurrente la extemporaneidad de una petición que había sido estratégicamente ocultada durante el desarrollo del proceso, invitando a aquélla a que fuera ya en el informe cuando se hicieran las alegaciones que se consideraran oportunas. En ese momento, sin exteriorizar protesta alguna, la defensa invocó el reconocimiento de los hechos por parte del acusado e interesó, con carácter subsidiario a la absolución que había sido pedida en conclusiones provisionales, la aplicación de los arts. 183.1 y 77 del CP .*
De ahí que lo que podía haberse formalizado como una pretensión que reclamara la ilicitud de un medio probatorio -no una causa de nulidad del juicio, como erróneamente se invocó por la defensa- fue degradado a la condición de argumento tardío, mezclado en el juicio oral con alegaciones de distinta naturaleza que, en último término, fueron explícita o implícitamente rechazados por el Tribunal de instancia».

[678] Dispone el precepto bajo la denominación de Impertinencia o inutilidad de la actividad probatoria que: «*1. No deberá admitirse ninguna prueba que, por no guardar relación con lo que sea objeto del proceso, haya de considerarse impertinente. 2. Tampoco deben admitirse, por inútiles, aquellas pruebas que, según reglas y criterios razonables y seguros, en ningún caso puedan contribuir a esclarecer los hechos controvertidos. 3. Nunca se admitirá como prueba cualquier actividad prohibida por la ley».*

[679] Vid. SANCHÍS CRESPO, Carolina. *La prueba por medios audiovisuales e instrumentos de archivo en la LEC 1/2000 (Doctrina, jurisprudencia y formularios)*. Tirant lo Blanch "abogacía práctica". Valencia. 2002. Pág. 32.

Las diligencias de investigación tecnológica analizadas están llamadas a convertirse en prueba durante en el enjuiciamiento, por ello, su adopción debe ajustarse a los criterios de admisión de la prueba que hemos manifestado, de manera que no se vean expulsadas del conjunto de pruebas que se practicarán ante el juez encargado de resolver. Por lo tanto, hay que insistir en que deben ser respetados todos los presupuestos legales que se exigen para su adopción, (como por ejemplo, los supuestos en los que estas diligencias son aplicables, el respeto de los plazos de duración o la debida motivación de la resolución), para que el resultado de la diligencia, esto es la información o los datos obtenidos, no quede expulsado del acervo probatorio que haya de ser valorado por el juzgador. De ahí que, desde el inicio de la instrucción del procedimiento se haya de procurar el cumplimiento de cualquier exigencia o elemento que pueda determinar que, bajo la aplicación del art. 283 LEC, este medio de prueba quede fuera del material probatorio a valorar.

En el caso de las diligencias de registro de dispositivos, la afectación del derecho al "entorno digital", o a cada uno de los derechos individuales que se recogen en el art. 18 CE, exige ser especialmente cuidadoso en el cumplimiento de los presupuestos de validez y licitud, porque de no hacerse así, la diligencia estaría viciada de nulidad y quedaría fuera del proceso y excluida de cualquier posibilidad de valoración.

Por lo tanto, la forma de proceder a la hora de apreciar el valor probatorio del resultado de estas diligencias es el siguiente: en primer lugar, hay que comprobar la validez del acceso a las fuentes de prueba, esto es, que el acceso a la información contenida en el dispositivo o la web se haya realizado cumpliendo con todas las exigencias y requisitos de validez previstos en la Ley. En segundo lugar, habrá que examinar el correcto empleo de los medios de prueba, y por consiguiente, analizar el modo en que la información o los datos obtenidos de la práctica de la diligencia han de acceder a las actuaciones. De manera que, si la información ha sido incluida correctamente, siguiendo las exigencias previstas en la norma procesal penal, la consecuencia que se derivará será la posibilidad de que el Juez encargado de la valoración de la prueba obtenida, mediante un examen racional, pueda llevarla a cabo y no la rechace.

La regla que rige la valoración de la prueba es la sana crítica. Esta expresión reivindica la facultad del juez encargado de resolver el conflicto planteado, para tomar todo el conjunto de pruebas que le han sido sometidas, y valorarlas conforme estime más oportuno, si bien en esta operación nunca debe apartarse de la lógica, la razón, y el contenido de las normas legales.

En este apartado se analizará si las diligencias de investigación electrónica encajan en el concepto de prueba electrónica que se recoge en la legislación civil, y qué presupuestos se han de cumplir para que pueda ser una prueba válida, que pueda incorporarse a las actuaciones, y sirva a la finalidad probatoria pretendida en el juicio oral. Por último, se analizarán los criterios que deben

servir para valorar el resultado de las diligencias practicadas, transformadas ya en pruebas durante la fase decisoria.

6.3.1. Valoración de la prueba electrónica.

La adaptación de la legislación española a las nuevas tecnologías es un hecho, que puede ser apreciado en la reforma del Código Penal que recoge nuevas tipologías delictivas en las que es indispensable el empleo de dispositivos electrónicos: el ciberbulling o ciber acoso, ciber estafas, grooming, phishing, etc. El uso de la tecnología en la comisión de delitos conlleva, como contrapartida, su empleo para combatirlos. El resultado derivado de la investigación debe ser plasmado en las actuaciones, y esta actividad persigue, como finalidad, llegar al enjuiciamiento, fase en la que todos los indicios son sometidos a valoración.

Las diligencias de investigación analizadas permiten recabar, registrar y analizar los datos contenidos en dispositivos electrónicos, páginas web, intercambio de archivos electrónicos, la localización geográfica de un determinado dispositivo para saber donde estuvo en un momento concreto del pasado, el análisis de documentos de textos, imágenes, etc. El empleo masivo de internet es otro modo de acreditación de hechos y circunstancias relacionadas con la investigación del delito[680]. El resultado derivado del examen de todos estos nuevos medios de generar información, que sirven para acreditar extremos que son discutidos en un proceso judicial, ha permitido que por parte de la doctrina se haya desarrollado una categoría conceptual denominada "prueba electrónica o tecnológica".

La doctrina ha ido elaborando una teoría sobre esta clase de pruebas para ser aplicada a los procesos de cualquier jurisdicción[681]. La prueba electrónica es *«toda información de valor probatorio contenida en un medio electrónico y transmitida por dicho medio»*[682]. Esta definición permite ser aplicada al resultado que se obtiene tras la realización de las diligencias de investigación electrónica que se han ido estudiando, y por ello los datos y la información que se encuentren en estos dispositivos puede tener valor en un proceso penal. Y es que no debe perderse de vista que, en estos casos, hay una información que está contenida en un medio electrónico y puede remitirse por un

[680] Este extremo también es destacado por Vid. DELGADO MARTÍN, Joaquin. *Investigación tecnológica y prueba digital en todas las jurisdicciones*. Wolters Kluwer. La LEY. Madrid. 2016. Págs. 38, 39 y 40.
[681] Vid. DELGADO MARTÍN, Joaquin. *Investigación tecnológica y prueba digital en todas las jurisdicciones*. Op. Cit. Pág. 35.
[682] Cfr. DELGADO MARTÍN, Joaquin. *Investigación tecnológica y prueba digital en todas las jurisdicciones*. Op. Cit. Pág. 42. El mismo autor ha mantenido esta definición en trabajos posteriores; véase Vid. DELGADO MARTÍN, Joaquín. *La prueba digital. Concepto, clases, aportación al proceso y valoración* (1). Diario La Ley, Nº 6, Sección Ciberderecho, 11 de Abril de 2017, Editorial Wolters Kluwer. Pág. 1.

medio de las mismas características, por lo que resulta incardinable dentro del concepto de prueba electrónica que manejamos.

El concepto de prueba electrónica se ha desarrollado partiendo de la regulación que ofrece la LEC en su artículo 299, considerándose que aquellos medios de prueba como internet *«debe ser incluído dentro del numerus apertus del art.299.3 LEC»*[683] , mientras que también se sostiene que hay que estar a la naturaleza del dato de que se trate en cada caso, es decir, habrá que tener en cuenta se trata de una imagen, un sonido o un documento para poder clasificarlo dentro de alguna de las categorías del art. 299.2 LEC. Todas estas clasificaciones tienen su importancia porque en el proceso civil rige una valoración diferenciada entre los documentos y los demás medios probatorios[684].

En el proceso penal lo que accede al proceso es tanto el soporte, esto es el dispositivo intervenido, como su contenido: datos, archivos e imágenes, interesando al proceso la traducción de todos esos datos, del lenguaje informático en el que vienen codificados, al lenguaje escrito o visual en que se convierten, con la ayuda de los expertos correspondientes, para resultar comprensibles para el juzgador.

Siguiendo la distinción entre fuente de prueba y medio de prueba se podría decir que el pen drive, el cd, el ordenador o la tablet, el smartphone, el servidor en el que se depositan datos en la nube, o incluso un router que contenga datos de acceso a internet pueden ser las fuentes de prueba. El medio de prueba, por su parte, lo será tanto el CD que se aporte con los datos y que puede ser objeto de una simple reproducción, como el informe pericial o el documento en el que los datos traducidos del lenguaje informático en el que estaban en el interior de esos dispositivos pasa a uno susceptible de ser analizado y valorado por el Juez y las partes. Sin olvidar que también podrá ser medio de prueba alguno de los enumerados en el art. 299.2 LEC, esto es *«los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso»*[685].

En el caso del proceso penal estas operaciones que describe el 299.2 LEC deben hacerse, si cabe, con las máximas cautelas, que excluyan cualquier duda sobre la autenticidad de su contenido y

[683] Cfr. COLOMER HERNÁNDEZ, Ignacio, «La prueba tecnológica», en GONZÁLEZ CANO, María Isabel (Dir), *La Prueba. Tomo I. La Prueba en el Proceso civil*. Tirant lo Blanch. Valencia. 2017.
[684] Vid. COLOMER HERNÁNDEZ, Ignacio. Op.Cit. Pág. 604.

[685] Cfr. DELGADO MARTÍN, Joaquin. *Investigación tecnológica y prueba digital en todas las jurisdicciones*. Op. Cit. Pág. 44.

sobre el modo de obtención[686]. Además, las pruebas electrónicas, como las demás, deben, conforme al art. 283 LEC ser pertinentes, útiles y lícitas[687].

La jurisprudencia define la pertinencia como la *«relación entre las pruebas y el objeto del proceso»*, y el juicio sobre esta categoría es «*exclusiva competencia de los Tribunales ordinarios, los cuales vienen obligados a explicitar y motivar las resoluciones en que rechacen las pruebas propuestas»*[688]. El art. 588 bis a, apartado 5 de la LECrim, exige un juicio de valoración al Juez acerca de la admisión de cualquier diligencia de investigación del Título VII, proceso de razonamiento y análisis acerca de la diligencia solicitada, en el que han de ponderarse y valorarse un elevado número de aspectos. Estos argumentos, juicios y razonamientos son susceptibles de servir, en el futuro momento del enjuiciamiento, como argumentos útiles que sirvan para avalar la pertinencia de su práctica, pero ya como prueba en el juicio oral. Es obvio que estamos ante dos momentos procesales distintos y con finalidades diferentes, y en los que intervienen dos juzgadores completamente distintos. Así, aunque el instructor no puede valorar un resultado que aún no se ha producido, aunque debe tener en cuenta la potencialidad que se deriva de la realización de la diligencia que se le solicita, y admitir en su valoración cuál pueda ser el posible resultado de la diligencia, basado en un juicio de proporcionalidad. Por el contrario, el Juez encargado del enjuiciamiento fundamenta la pertinencia de la prueba, así como su posible relevancia, entendida jurisprudencialmente como la *«potencialidad para modificar de alguna forma importante el sentido del fallo»*[689], en los indicios dados durante la instrucción, y que sirven a las partes para que les sirvan como medios de prueba. Es por ello que, si bien proporcionalidad y pertinencia no son conceptos sinónimos, puede decirse que el segundo puede descansar en el conjunto de razonamientos seguidos para determinar la concurrencia del primero, pues resultaría extraño que la diligencia que se estimó como proporcionada por el juez instructor, y cuya practica se acordó, no fuera más tarde considerada como prueba pertinente por el tribunal encargado de resolver.

---

[686] Por ejemplo en la STS 754/2015, de 27 de noviembre. Ponente: Don Artemio Sánchez Melgar se hace alusión a la existencia de pantallazos que sirven para acreditar una conversación mantenida entre dos sujetos mediante el uso de mensajería instantánea. En este caso el TS aborda el hecho diciendo que se trata de una prueba, si bien debe ser tenida en consideración con todas las cautelas posibles dado la posibilidad de ser manipulada. Dice el texto de la sentencia que debe ser la parte que la aporta y quien trata de valerse de ella quien deberá acreditar su autenticidad e integridad mediante la aportación del informe pericial oportuno.

[687] En materia de prueba electrónica Vid. DELGADO MARTÍN, Joaquin*. Investigación tecnológica y prueba digital en todas las jurisdicciones*. Op. Cit. Pág. 47, analiza estos conceptos aplicados a la prueba electrónica considerando que la licitud ha de atribuirse al medio de obtención de la prueba, la pertinencia y necesidad son atribuciones propias del método de inclusión de tales diligencias en el proceso, siendo la observancia de los requisitos procesales para hacerlo un aspecto más de la propia acción de inserción en el proceso mismo. Por último señala la valoración como el último de los eslabones propios de la prueba digital.

[688] Sirva de ejemplo la STS 1140/2010 de 29 de diciembre. Ponente: Don Juan Ramón Berdugo y Gómez de la Torre. La resolución repasa en su fundamento de derecho décimo primero estos requisitos.

[689] STS, 807/2014, de 2 de diciembre de 2014. Ponente: Don Miguel Colmenero Menéndez de Luarca.

El concepto de utilidad del art. 283 LEC, se relaciona por parte la jurisprudencia con la necesidad de la práctica de dicha prueba. Se define como útil algo que resulta beneficioso o provechoso, por lo tanto, la utilidad de la prueba irá relacionada con el provecho que dicha prueba conlleva para la parte proponente. No obstante, esa utilidad subjetiva o de parte, no tiene que guardar relación con la utilidad que pueda apreciar el tribunal[690].

El tercer requisito que debe reunir la prueba es la licitud. En el proceso penal es lícita la prueba practicada conforme a la LECrim y la jurisprudencia. Es decir, evitando cualquier vulneración de derechos fundamentales y realizada conforme a sus leyes reguladoras. El concepto se contrapone al de prueba ilícita que tanto ha estudiado la jurisprudencia [691].

En el caso del acceso a los dispositivos de almacenamiento masivo de información, y más si cabe, en la diligencia de acceso remoto a un ordenador, los derechos fundamentales, se ven muy afectados. Esta limitación se salva observando escrupulosamente los requisitos de la LECrim para su correcta aplicación. Este aspecto determina la legalidad de la diligencia durante la instrucción y posteriormente su admisibilidad como prueba, porque si no se obtuvo válidamente, las consecuencias que se derivan de la aplicación del art. 11.1 de la LOPJ, y de la doctrina "*de los frutos del árbol envenenado*" [692], matizada por la tesis de la "conexión de antijuridicidad" [693], supone dejar sin efecto las pruebas que lesionaron los derechos en juego y también las que se derivaron directamente de ellas, si bien admitiendo las que se desvinculan del origen ilícito de la primera.

---

[690] La STS, 759/2014, de 25 de noviembre de 2014. Ponente: Don Juan Ramón Berdugo y Gómez de la Torre, específica que *«la prueba sea además, necesaria, es decir tenga utilidad para los intereses de defensa de quien le propone».* Sigue diciendo el texto de la sentencia que: *«A diferencia de la pertinencia que se mueve en el ámbito de la admisibilidad como facultad del tribunal, la necesidad de su ejecución se desenvuelve en el terreno de la práctica, de manera que medios probatorios inicialmente admitidos como pertinentes pueden lícitamente no realizase, por muy diversas circunstancias que eliminen de manera sobrevenida su condición de indispensable y forzosa, como cualidades distintas de la oportunidad y adecuación propias de la idea de pertinencia».*

[691] Sirva como ejemplo la STS 53/2011, de 10 de febrero de 2011. Ponente: Don Juan Ramón Berdugo y Gómez de la Torre. La resolución repasa el concepto de prueba ilícita y el destino que debe darse a la misma conforme al contenido del art. 11.1 de la LOPJ.

[692] La doctrina de los frutos del árbol envenenado implica esencialmente la imposibilidad para el Juez no ya solo de valorar las pruebas que se han obtenido vulnerando derechos fundamentales, lo que resulta un mandato expreso del art. 11.1 LOPJ para los casos de obtención con violación directa o indirecta de los derechos fundamentales, sino que conlleva extender esa imposibilidad de valoración hasta las pruebas que se han obtenido de manera derivada de aquellas iniciales que han sido tenidas por nulas. Sobre este particular se puede consultar Vid. PICÓ I JUNOY, Joan. «Nuevas perspectivas sobre el alcance anulatorio de las pruebas ilícitas». *Diario La Ley*. 1997. LA LEY 11968/2001 I. Pág. 5 a 9. También Vid. LÓPEZ RAMÍREZ, Antonio. *La prueba ilícita penal*. Tirant lo Blanch. Ciudad de Méjico. 2019. Pág. 265

[693] Vid. GARRIDO LORENZO, M. Ángeles. «Valoración en el juicio oral de la prueba y conexión de antijuridicidad» *Diario La Ley*, Nº 7573, 21 de Febrero de 2011. La Ley 1829/2011. Págs. 1 a 3.

6.3.2. La libre valoración de la prueba.

La valoración de la prueba es una actividad que consiste en realizar un juicio en el que se exteriorice la opinión que le merecen al Juez las pruebas practicadas en las actuaciones y el resultado obtenido con las mismas. Esta actividad del juzgador es realizada de un modo racional y lógico, de modo que ese juicio valorativo sobre la eficacia de las distintas pruebas practicadas ha de servir para sostener la decisión que finalmente adopte sobre la *quaestio facti* objeto del proceso. Es tan importante el proceso valorativo, y su resultado, que cuando el mismo no se sigue adecuadamente, de manera que se aprecie que no es lógico el razonamiento seguido en dicha valoración, se configura esta circunstancia como un motivo para poder recurrir a instancias superiores. De hecho, las normas reguladoras de las diferentes tipologías de recurso aluden, con los matices propios de las características de cada recurso en cuestión, expresamente a la errónea valoración de la prueba como uno de los posibles motivos a esgrimir en la interposición de éstos[694].

Las diligencias de investigación electrónica también son objeto de valoración, que debe ponerse en relación con las demás pruebas del proceso, y el modo racional de relacionarlas entre sí debe conducir a sostener si el fallo en el que se aprecie la culpabilidad o inocencia del sujeto activo. El objeto concreto a ser valorado son los datos que se obtuvieron como consecuencia de la practica de un registro de datos electrónicos.

En orden a la valoración de las pruebas hay dos posibilidades: una de ellas implicaría que las reglas de valoración se encuentren expresamente reguladas en la ley, ejecutando dicho acto de valoración conforme a ellas, que es lo que se denomina «*valoración legal*». La otra posibilidad consiste en la llamada «*libre valoración*»[695], que permite al órgano judicial decisor valorar las pruebas que le son sometidas de forma completamente libre de cualquier esquema previo. La libre valoración implica que el Juez o Tribunal no verá sometido a ningún condicionante, supeditación o limitación, mas que a la lógica, la razón y el examen minucioso de las pruebas que se le presentan. Ahora bien, pese a esta enorme amplitud jurisdiccional a la hora de valorar la prueba *«el juzgador no puede llegar a un juicio de culpabilidad fundándose en cualquier elemento incriminatorio, con independencia de su finalidad, según las reglas de la lógica y la razón»*[696]. Es decir, el Juez cuenta con una muy importante libertad a la hora de abordar la valoración del conjunto de prueba que se aportan al

[694] Así lo dispone el art. 790.2 LECrim con respecto al recurso de apelación, o el art. 849.2º LECrim en los casos de valoraciones erróneas efectuadas sobre documentos obrantes en las actuaciones, que son literosuficientes, esto es, que no son contradichos por otros medios.
[695] Cfr. IGARTUA SALAVERRÍA, Juan. *Valoración de la prueba, motivación y control en el proceso penal*. Tirant lo Blanch. Valencia 1995. Pág. 32.
[696] Cfr. MORENO CATENA, Víctor. *Derecho Procesal Penal*. Tirant lo Blanch. Valencia. 2019. Pág. 442

proceso, pero al mismo tiempo no puede confiar dicha valoración a su propia subjetividad, por más apariencia lógica que esta posea.

El criterio de libre valoración de las pruebas es el que sigue el Derecho español y se refleja en las normas del proceso civil y del proceso penal.

En el proceso penal se aplica la regla de libre valoración y se denomina valoración en conciencia de la prueba (741 LECrim)[697]. La valoración de la prueba penal debe ajustarse a un examen racional, lógico y epistémico, basado en el examen racional del conjunto de pruebas traídas al proceso, puestas todas ellas en conjunta consonancia y contradicción, y cuyo fundamento legal está principalmente en el art. 741 LECrim. Además, la actividad valorativa deberá verse complementada con un importante esfuerzo y diligencia en la motivación, que no es sino una exigencia derivada del propio texto constitucional (art. 120. CE)[698].

La motivación requiere que se expliquen y razonen las conclusiones acogidas respecto del resultado de cada uno de los medios probatorios propuestos por las partes [699], porque la explicación de las razones que justifican la decisión del juzgador sobre el valor probatorio de toda prueba practicada es la que permite que otros órganos superiores puedan controlar, por la vía de los recursos pertinentes, la corrección de la decisión judicial.

Esta libertad no debe verse constreñida mas que por el examen racional y lógico de los hechos. Ahora bien, esta libertad valorativa del juzgador en relación con las pruebas no puede significar que su decisión se desvíe hacia la discrecionalidad o la arbitrariedad, ya que esto supondría incurrir en un vicio que podría determinar el acceso a la casación y la revocación de la resolución en la que se diera esta circunstancia.

La libertad en la valoración de las pruebas penales es un axioma que se recoge en los arts. 741 y 973 LECrim. Ante una regulación tan escasa, ha sido el Tribunal Constitucional el que ha ido configurando esta facultad, conjugando el respeto de una serie de presupuestos, pero siendo escrupuloso con la facultad judicial que comporta la comparación, ponderación, reflexión, estudio, análisis y extracción de consecuencias lógicas de los distintos elementos probatorios que se le someten.

---

[697] Vid. GONZÁLEZ CANO, M. Isabel y FIDALGO GALLARDO, Carlos. «Valoración de la prueba, presunción de inocencia y principio in dubio pro reo» en ROMERO PRADAS, M. Isabel (Dir) y GONZáLEZ CANO, M. Isabel. *La Prueba. Tomo II. La prueba en el proceso penal*. Tirant lo Blanch. 2017, Pág. 440.

[698] Vid. COLOMER HERNÁNDEZ, Ignacio. La motivación de las sentencias: sus exigencias constitucionales y legales. Tirant lo Blanch. Valencia. 2003. Pág. 95.

[699] Así lo mantiene Vid. ZUBIRI DE SALINAS, Fernando. «¿Qué es la sana crítica?. La valoración judicial del Dictamen de experto». *Revista de Jueces para la democracia información y debate*. nº 50, año 2004. págs. 52-62. En concreto, sobre el aspecto particular de la valoración de las pruebas, hago remisión al contenido obran en la pág. 54.

El Tribunal Constitucional exige, en primer lugar, que se realice una actividad probatoria de cargo, lo que implica que la prueba que se practique, una vez valorada, apunte necesaria e insoslayablemente desde una perspectiva lógico racional hacia la decisión adoptada. En este sentido, se requiere que la prueba conduzca a la conclusión lógica de que el acusado es el responsable de la comisión del ilícito penal que se somete a enjuiciamiento[700]. El Tribunal Constitucional requiere tan solo que, con carácter previo, existan elementos probatorios en la causa, para evitar una condena sin pruebas, lo que indudablemente atentaría contra el principio de presunción de inocencia[701].

La justicia internacional también exige la presencia de elementos probatorios previos, que deben ser analizados para ver si concurre algún elemento que fundamente la condena. Este aspecto determina o no la observancia de los tratados internacionales que protegen los derechos humanos y las libertades fundamentales. En esto también coincide nuestro Tribunal Constitucional que exige la presencia de elementos probatorios que apunten a la presunta culpabilidad del sujeto. El material probatorio debe ser suficiente para fundamentar un pronunciamiento que desvirtúe la presunción de inocencia y que además esté fundado en verdaderos actos de prueba[702].

El segundo aspecto que exige el Tribunal Constitucional es exigir que la actividad probatoria se realice con respeto a todas las garantías, sin perjuicio del respeto a las demás garantías del proceso como por ejemplo el derecho a ser informado de la acusación, el derecho de defensa y contradicción, el de estar presente en el juicio, el derecho a un tribunal imparcial o el derecho a la

---

[700] La STS de 4 de abril de 1989. Ponente: D. Francisco Soto Nieto, señalada igualmente por Cfr. IGARTUA SALAVERRÍA. Op. Cit. Pág. 93, pone acento en esta materia cuando dice que para la existencia de prueba de cargo no basta con su simple existencia, lo cual es presupuesto necesario, sino que además la misma ha de constituir una *«actividad probatoria capaz de montar sobre ella el andamiaje lógico y jurídico de una inculpación fundada, antecedente y paso de la responsabilidad reconocida y decretada, siempre haciendo uso de su soberano criterio y de la llamada a la conciencia y a la racionalidad que efectúan los artículos 717, 741 y 973 de la Ley Procesal Penal».*

[701] Si analizamos resoluciones del TEDH podemos concluir con que existen un elevado número de decisiones de inadmisión de demandas de vulneración del derecho a la presunción de inocencia. En este sentido se constata que el Tribunal Europeo suele amparar su decisión de inadmisión en la apreciación que efectúa sobre la existencia o no de acervo probatorio. Así hay que recordar que el derecho a la presunción de inocencia se recoge en el art. 6.2 del Convenio Europeo de derechos humanos, y entre las resoluciones de inadmisión citaremos: Decisión del Tribunal Europeo de Derechos Humanos (Sección 4ª) de 15 diciembre 1998. Caso A.E.D.L.G contra España *«el Tribunal constata que tanto la Audiencia Nacional como el Tribunal Supremo basaron sus sentencias en motivos de derecho y en unos elementos de hecho que consideraron suficientes, como para llegar a la conclusión de la declaración de culpabilidad del demandante";* la decisión del Tribunal Europeo de Derechos Humanos (Sección 4ª), de 18 de octubre de 2005, Caso Roldán Ibáñez contra España, en la que se dice: *«el Tribunal a quo dispuso de pruebas a cargo, tanto en lo que concierne a las declaraciones de los testigos como en lo que concierne a los peritajes. Estas pruebas fueron presentadas durante el proceso conforme a las garantías de inmediatez, de oralidad y de publicidad. Así mismo, fueron apreciadas [por la Audiencia Provincial] de manera suficientemente motivada».* Por último se cita la decisión del 7 de septiembre de 2010 Tribunal Europeo de Derechos Humanos (Sección 3ª). Caso Fernández Saavedra contra España.

[702] STC 17/2002 de 28 enero. Ponente: Doña Elisa Pérez Vera. En la sentencia resulta ilustrativo que al determinar el contenido y alcance del principio de presunción de inocencia se señala que el mismo *«entraña el derecho a no ser condenado sin pruebas de cargo válidas*». Y que además, deba hacerse indicación expresa de las pruebas tenidas en cuenta para fundar una condena.

última palabra[703]. El respeto a las garantías exigibles a la actividad probatoria implica que ésta se realice durante el juicio[704], momento en el que deben respetarse los principios de inmediación, oralidad, concentración y contradicción[705], y por último se insta a que todo el acervo probatorio sometido a valoración se haya obtenido sin violentar derechos fundamentales[706].

El examen del correcto discurrir la valoración de las pruebas obrantes en las actuaciones, desde la fase de instrucción hasta la vista oral, implica ir desgranando, con entera libertad de criterio, si concurren todos estos aspectos anteriormente expuestos en sentido positivo o negativo. Si faltase alguno de ellos, o existiendo, no se ajustaran al canon de interpretación racional, deberá ser expulsado del acervo probatorio en los casos de vulneraciones a los derechos fundamentales[707], y en los demás casos deberá motivarse en la resolución las razones por las que la prueba no se tiene en consideración.

---

[703] Ver como ejemplo la STEDH (Sección 1ª), de 26 marzo 2015, Caso Volkov y Adamskiy contra Rusia, en la que se valora como uno de los elementos integrantes del derecho al proceso con todas las garantías que se integra en el art. 6.1 del CEDH el derecho de defensa. La STEDH (Sección 3ª), de 11 octubre 2016, Caso Iglesias Casarrubios y Cantalapiedra Iglesias contra España considera como parte integrante de un proceso equitativo, el derecho a la contradicción.

[704] Excepción hecha de la prueba preconstituída y anticipada, que a pesar de haberse realizado en la fase de investigación deberán incorporarse al juicio oral con todas las garantías y requisitos legalmente previstos.

[705] Estos principios también se integrarían dentro del derecho a un proceso con todas las garantías, así se extrae de la STC 30/2010, de 17 de mayo. Ponente**:** Doña Elisa Pérez Vera, que estableció que *«....el respeto a los principios de publicidad, inmediación y contradicción, que forman parte del contenido del derecho fundamental invocado, impone inexorablemente que toda condena articulada sobre pruebas personales se fundamente en una actividad probatoria que el órgano judicial haya examinado directa y personalmente en un debate público, en el que se respete la posibilidad de contradicción....».*

[706] Sobre este aspecto aludiremos a las STC 126/1986 de 22 de Octubre, Ponente: Don Francisco Rubio Llorente, STC 25/2003 de 10 de febrero, Ponente: Doña Elisa Pérez Vera (estas aluden principalmente a que dicha función valorativa del art. 741 LEcrim es exclusiva del Juzgador), y a la STC 31/1981, de 28 de Julio. Ponente: Doña Gloria Begue Cantón. En esta última resolución se dice sobre la facultad de libre valoración que: *«El principio de libre valoración de la prueba, recogido en el art. 741 de la L. E. Crim., supone que los distintos elementos de prueba puedan ser ponderados libremente por el Tribunal de instancia, a quien corresponde, en consecuencia, valorar su significado y trascendencia en orden a la fundamentación del fallo contenido en la Sentencia. Pero para que dicha ponderación pueda llevar a desvirtuar la presunción de inocencia, es preciso una mínima actividad probatoria producida con las garantías procesales que de alguna forma pueda entenderse de cargo y de la que se pueda deducir, por tanto, la culpabilidad del procesado, y es el Tribunal Constitucional quien ha de estimar la existencia de dicho presupuesto en caso de recurso. Por otra parte, las pruebas a las que se refiere el propio art. 741 de la L. E. Crim., son «las pruebas practicadas en el juicio», luego el Tribunal penal sólo queda vinculado a lo alegado y probado dentro de él (secundum allegata et probata)».*

[707] Deseo reproducir las palabras de la STS más arriba mencionada de 4 de abril de 1989. Ponente: D. Francisco Soto Nieto, y cuyo fundamento segundo es, en parte, también mencionado en IGARTUA SALAVERRIA. Op. Cit. Pág. 93: *«La estimación «en conciencia» de las pruebas a que alude el artículo 741 de la Ley Procesal Penal no ha de entenderse ni hacerse equivalente a cerrado e inabordable criterio personal e íntimo del juzgador, sino a una apreciación lógica de la prueba, no exenta de pautas o directrices de rango objetivo, fiel a los principios del conocimiento y de la ciencia, a las máximas de la experiencia, a las reglas de la sana crítica, que aboque en una historificación de los hechos en adecuado ensamblaje con ese acervo de mayor o menor amplitud, de datos acreditativos o reveladores, que haya sido posible concentrar en el proceso».* Se trata de un resumen del modo en que debe ser entendido el contenido del art. 741 LECrim. Se trata de una posibilidad valorativa que entremezcla razón con convencimiento; intuición y lógica; material objetivo derivado de las actuaciones, con convicción personal. En todo caso el autor citado considera sujeto a crítica el sistema de valoración de prueba expuesto.

Este hecho último comportará que la prueba no sea tenida en consideración, no se valore, lo que la expulsará del acervo de pruebas existente, y como consecuencia de ello, y llegado el caso, podría suponer la completa absolución del procesado.

En el caso de las diligencias de investigación electrónica una correcta valoración supondrá examinar si la autorización de su práctica se ajustó a los nuevos presupuestos que exigen los arts. 588 sexies y 588 septies LECrim. Esto implica que se ha de analizar el respeto a los presupuestos y situaciones que se exigen para su adopción, realizar una valoración sobre la suficiencia de la motivación, especialmente en lo que se refiere al canon de proporcionalidad. El desajuste de la medida a algunos de los requisitos mencionados puede comportar la nulidad de dichas diligencias, y como consecuencia de ello el que resulten apartados del proceso y de su valoración los datos obtenidos en ella.

Debe tenerse en cuenta, además, las posibilidades de contradicción efectiva por las defensas, y el modo en que dicha contradicción se lleva a cabo (por ejemplo, proponiendo análisis periciales contradictorios, o pruebas testificales que pongan en duda el contenido de las diligencias practicadas). En este sentido, habrá que analizar si la incorporación del resultado de la diligencia de investigación electrónica al procedimiento se ha llevado a cabo de forma correcta, y si se ha vuelto a reproducir posteriormente en la vista oral.

Por último, la valoración de estas diligencias debe ser coherente con el sentido de la sentencia. Se trata de ofrecer un examen racional, y aportar una consecuencia lógica. La diligencia ha de tomarse en consideración no sola o aislada, sino en un contraste suficientemente valorado con respecto al resto de pruebas aportadas y practicadas en las actuaciones. De manera que de la comparación y del valor dado a cada prueba por el juzgador es de donde se debe extraer el fundamento o justificación que apoye la decisión de condena o de absolución, sin que tenga que influir sobre tal decisión el hecho de que una o varias de las pruebas traídas al proceso tengan naturaleza tecnológica[708], ya que lo determinante es el resultado al que dichas pruebas conducen y no el soporte o medio en el que son aportadas.

El acusado ha debido participar en el desarrollo del proceso ofreciéndosele directamente la posibilidad de que se pronuncie sobre el contenido de la diligencia, lo cual es perfectamente admisible en el trámite del derecho a la última palabra [709], que no debe perderse de vista que es un

[708] Vid. ARRABAL PLATERO, Paloma. *La prueba tecnológica: aportación, práctica y valoración.* Tirant lo Blanch. Valencia. 2020.Pág. 417.

[709] El derecho a la última palabra es un derecho especialmente conferido al acusado, así lo sostiene el voto particular efectuado por el Magistrado D. Joaquín Jiménez García, dentro de la STS 556/2017, de 13 de julio, que confiere al acusado la posibilidad de poder pronunciarse sobre cualquiera de los aspectos en los que se funda su acusación, según se mantiene en la STS 228/2018, de 17 de mayo. Ponente: Doña Ana María Ferrer García, por citar de las más recientes.

derecho integrado en el derecho de defensa, y que sirve para que el investigado-acusado pueda pronunciarse sobre los aspectos de la vista y de todo lo que en ella ha sucedido.

En suma, si todos estos requisitos son respetados y observados, no debe existir inconveniente para que el resultado de la práctica de cualquiera de las diligencias de investigación electrónica sirva como prueba de cargo que desvirtúe el principio de presunción de inocencia de todo ciudadano. En consecuencia, la diligencia puede ser el fundamento del dictado de una sentencia condenatoria. Por el contrario, si la convicción derivada de éstas y otras diligencias no alcanza para desvirtuar el citado principio de presunción de inocencia, la desestimación de las pretensiones de condena deducidas contra el acusado, debe ser la decisión racional que debe adoptar el juzgador.

Es un derecho que, dado su alcance constitucional, ha sido objeto de varias resoluciones por dicho tribunal. Destaca por su sencillez y claridad la mencionada en la STC 93/2005, de 18 de abril. Ponente: Don Roberto García Calvo y Montiel y a cuyo tenor, «*el derecho a la defensa comprende, en este aspecto, no sólo la asistencia de Letrado libremente elegido o nombrado de oficio, en otro caso, sino también a defenderse personalmente [arts. 6.3 c) y 14.3 d) del Convenio y del Pacto más arriba reseñados] en la medida en que lo regulen las leyes procesales de cada país configuradoras del derecho. Es el caso que la nuestra en el proceso penal (art. 739 LECrim) ofrece al acusado el 'derecho a la última palabra' (Sentencia del Tribunal Supremo de 16 de julio de 1984), por sí mismo, no como una mera formalidad, sino -en palabras del Fiscal que la Sala asume- 'por razones íntimamente conectadas con el derecho a la defensa que tiene todo acusado al que se brinda la oportunidad final para confesar los hechos, ratificar o rectificar sus propias declaraciones o las de sus coimputados o testigos, o incluso discrepar de su defensa o completarla de alguna manera'. La raíz profunda de todo ello no es sino el principio de que nadie pueda ser condenado sin ser oído, audiencia personal que, aun cuando mínima, ha de separarse como garantía de la asistencia letrada, dándole todo el valor que por sí misma le corresponde. La viva voz del acusado es un elemento personalísimo y esencial para su defensa en juicio».*

7. Conclusiones.

Con la exposición de todo lo anterior puede considerarse finalizado este estudio, y con ello el examen de los distintos aspectos y derechos afectados por las diligencias de investigación tecnológica consistentes en el acceso a dispositivos de almacenamiento masivo de información y el acceso remoto a equipos informáticos.

Ha sido analizado el contenido de la normativa reguladora de cada una de estas diligencias, y se ha expuesto, especialmente la problemática derivada del acceso a los sistemas informáticos que, gestionados por terceros, albergan información de interés para la investigación criminal en la nube.

Por todo eso, y una vez completada la redacción de este trabajo y expuesto en el contenido del mismo todas las variables y consideraciones que se han estimado relevantes, se hace necesario realizar, a continuación, una exposición de manera resumida y breve de aquellas principales conclusiones alcanzadas sobre los problemas analizados.

PRIMERA

La entrada en vigor de la reforma de la LECrim sobre diligencias de investigación electrónica, ha supuesto la introducción en nuestro ordenamiento de una regulación en la que se contiene un tratamiento procesal integral que aúna la protección de los derechos del art. 18 CE con el empleo de medios tecnológicos aplicados a la investigación penal.

El Título VIII, del Libro II de la LECrim contiene una regulación integral de las diligencias o medidas de investigación que afectan o limitan a los derechos contemplados en el art. 18 CE.

En general cada diligencia que se regula dentro de ese título se corresponde exclusivamente con uno derecho de los comprendidos dentro del art. 18. Pero esta regla de exclusividad no se cumple en el caso de las diligencias de investigación reguladas en los Capítulos VIII y XI del Título VIII del libro II de la LECrim, ya que son las únicas en las que se puede ver afectado más de un derecho de los contenidos en el art. 18 CE, incluso de forma simultánea.

La limitación conjunta de varios derechos constitucionales que se puede producir durante la práctica de alguna diligencia de investigación electrónica, ha sido el origen del desarrollo de la doctrina del

llamado derecho al propio entorno virtual o digital, que ha sido acogida por la jurisprudencia. Esta doctrina cristaliza en la creación de un nuevo derecho que implica, a efectos prácticos, que se necesite una autorización judicial para adoptar cualquier medida de investigación electrónica en la que se puedan limitar varios de los derechos fundamentales del art. 18 CE que, aisladamente considerados, no hubieran exigido la concurrencia de dicha autorización judicial para ello, por no venir exigido por el texto constitucional. Esta doctrina equipara todos los derechos del art. 18 CE haciendo insoslayable la garantía de intervención judicial y ponderación de los intereses en conflicto.

El reconocimiento de este derecho es un importante avance en la defensa de los derechos fundamentales del art. 18 CE y supone una equiparación y un tratamiento homogéneo para cualquier clase de limitación sobre ellos derivada de una actuación penal. El texto de la LECrim se hace más protector que el propio texto constitucional cuando se trata de proteger algunos de estos derechos.

Es aconsejable que una futura reforma del texto constitucional equipararse todos los derechos del art. 18 CE para unificar el criterio que en la actualidad exige la jurisprudencia y el texto de la LECrim, porque mientras el art. 18 CE no requiere intervención judicial en todos los casos, la LECrim si lo hace cuando sea posible que con la diligencia de investigación que se pretende llevar a cabo pudieran afectarse más de uno de los derechos del art. 18 CE de manera simultánea.

SEGUNDA

La producción de legislación nacional e internacional sobre el tratamiento y el uso de la tecnología en la comisión de delitos y en el modo de investigarlos se ha incrementado.

La tecnología presenta ventajas indiscutibles. A nivel jurídico procesal, y en concreto en el ámbito penal, podemos destacar dos aspectos:

1.- Existe una creciente actividad legislativa internacional tendente a regular medidas de investigación tecnológica de todo tipo, que va más allá de la consistente en la intervención de las comunicaciones postales o telefónicas. Esta legislación internacional, ratificada por España, pone el acento en la intervención de comunicaciones, en la captación de datos electrónicos de interés para una investigación criminal, y en la legislación sobre la investigación de delitos de trascendencia

económica. Destaca en este orden, en el ámbito de la Unión Europea, la creación de un órgano especializado denominado Fiscalía Europea, cuyo fin es coordinar la investigación penal de estos delitos, así como la creación de instrumentos que permitan la ejecución de diligencias de investigación en otros países miembros de la UE.

2.- La actividad legislativa nacional en materia penal, enriquecida por la recepción de las normas internacionales, se caracteriza por la creación de nuevos tipos penales cuyo tipo objetivo contiene modalidades comisivas consistentes en la realización de actos con un componente netamente informático, o en el que predomina el uso de la tecnología. Esto lleva aparejada la necesidad de que se regulen diversas modalidades de investigación basadas igualmente en el empleo de la tecnología, que conjuguen la necesidad de tener conocimiento de la existencia del hecho delictivo, de su modo de ejecución, sus participantes, así como conseguir con ello su persecución y una mejor investigación, conjugando todo ello con el respeto a los derechos fundamentales, que es un aspecto que constituye el fundamento de las sociedades avanzadas.

TERCERA

Las diligencias de investigación electrónicas son susceptibles de ser clasificadas.

La Ley realiza una enumeración de las diferentes diligencias de investigación electrónica que limitan cada uno de los derechos del art. 18 CE. La diversidad de diligencias recogidas en la Ley permite realizar una propuesta de clasificación de las medidas de investigación contenidas en el Título VIII de la LECrim, basada en distintos criterios, pero cuyo punto de partida es siempre el texto legal.

Una primera propuesta de clasificación atendería al tipo de derecho fundamental afectado por la diligencia, es decir, si la diligencia afecta a la intimidad, al secreto de las comunicaciones, a la inviolabilidad del domicilio, a la propia imagen, etc. La jurisprudencia admite que la práctica de una medida de investigación conlleve la limitación de varios derechos del art. 18 CE al mismo tiempo, sin que predomine en dicha limitación un derecho sobre los demás, porque todos se ven afectados a la vez. Este hecho ha originado la doctrina de la sala segunda del Tribunal Supremo que constituye el origen del nuevo derecho llamado “derecho al propio entorno digital o virtual”.

Una segunda propuesta clasificatoria viene dada por la exigencia de mayores o menores presupuestos legales para la adopción, de forma que existen diligencias que exigen una serie de

requisitos generales, que son aplicables a todas de manera general, mientras que otras exigen aspectos únicos y exclusivos.

Una tercera propuesta de clasificación permite diferenciar las diligencias de investigación reguladas en la LEcrim atendiendo a su carácter originario o derivado, es decir, las que suelen ser origen o inicio de la instrucción penal, o las que son derivadas de otras diligencias anteriores, en orden a complementar, reforzar o posibilitar una mejor comprensión de los hechos que se instruyen.

CUARTA

La regulación procesal penal española sobre diligencias de investigación tecnológica ha sido formulada tardíamente y está influenciada por diversos instrumentos internacionales que han determinado expresamente su contenido. El resultado obtenido es una legislación avanzada y de las más variadas y completas de su entorno geográfico y cultural. Permite el acceso y registro de datos en la nube, si bien con importantes carencias técnicas en aspectos relevantes que afectan a la propia jurisdicción, y sobre las que no se pronuncia. La redacción legal de las diligencias de registro de dispositivos y de registro remoto ofrece un relevante consenso que augura estabilidad y perdurabilidad.

1.- En España la regulación de las medidas de investigación tecnológica ha sido tardía, lo que le ha valido críticas. No obstante, la regulación vigente es abundante, variada y prolija comparada con las legislaciones nacionales de otros estados.

La tramitación legislativa de las diligencias que permiten el acceso y el registro de los datos contenidos en dispositivos de almacenamiento masivo de información y la que faculta el acceso remoto a equipos informáticos, suscitó muy escasa controversia, centrándose el poco debate legislativo sobre estas diligencias en la posibilidad de adoptar las medidas por los investigadores amparada en razones de urgencia y con la necesidad de que se produzca una ratificación judicial inmediata.

El acuerdo de la mayor parte de los grupos parlamentarios sobre la necesidad de regulación de este tipo de diligencias aventura que no verá modificado su contenido sustancialmente en el futuro, contribuyendo así a una mejor aplicación de su contenido y de su desarrollo jurisprudencial.

2.- El Convenio de Budapest sobre Ciberdelincuencia es el instrumento internacional que ha influido en el contenido de la regulación española vigente. El Convenio exige a los países firmantes

que incluyan en sus legislaciones tanto ciertas diligencias de investigación electrónica como ciertos tipos penales. En los países de nuestro entorno existen regulaciones tendentes a posibilitar el acceso a dispositivos informáticos en los que queda alojada información útil a la investigación criminal, pero puede decirse que la legislación española es la más rica y variada de todas las analizadas en este sentido.

La Directiva 2014/41/CE del Parlamento Europeo y del Consejo de 3 de abril de 2014, relativa a la orden europea de investigación en materia penal, permite que las diligencias de acceso a dispositivos de almacenamiento de información (entre las se incluye el registro a dispositivos en la nube) sean ejecutadas por diferentes países de la UE a requerimiento de la autoridad competente de otro. Esto sucederá siempre que la práctica de esas diligencias esté prevista expresamente en la legislación de dicho país, o exista alguna diligencia similar que permita hacerlo, y cuya necesidad de ejecución sea valorada y ponderada de manera adecuada, suficiente y proporcional.

La creación de la Fiscalía Europea ahonda en el Espacio de Seguridad y Justicia común. Entre las facultades de esta Fiscalía está solicitar la ejecución de diligencias de investigación previstas en nuestro ordenamiento. Las normas que regulan esta Fiscalía permiten el acceso a datos encriptados y almacenados, sin que se plantee cuestión alguna en su regulación acerca del lugar físico en que los datos se encuentran, lo que permite concluir que el Fiscal europeo puede, si la legislación procesal nacional lo permite, pedir que se registren datos alojados en la nube con independencia de su ubicación, mientras que esté dentro del territorio de los países adscritos a la creación de este organismo. Esta posibilidad, por el contrario, no se permite en nuestra legislación, que no hace mención a cuestión territorial alguna, y tampoco desarrolla claramente los diferentes modos de acceso a los datos en esos casos de ausencia de seguridad sobre la ubicación de los datos.

QUINTA

La legislación procesal penal no define el concepto de dato. Es un concepto que ha de extraerse de la legislación específica que los regula y del objeto del proceso. En todo caso, el concepto de dato, a los efectos procesales penales, es tan amplio como lo exija el objeto del procedimiento, abarcando cualquier dato electrónico que resulte de interés para la investigación. En todo caso, para su acceso y su análisis habrá de estarse a la naturaleza de dicho dato, a si su acceso comporta la vulneración de algún derecho constitucional, a la legislación procesal penal que determina el acceso y a la normativa que regule de manera general la conservación y el acceso a dichos datos.

El concepto de dato, entendido como la información que se obtiene tras la práctica de las diligencias de investigación tecnológica tanto de acceso a dispositivos de almacenamiento masivo de información, como de acceso remoto a equipos informáticos, no se encuentra regulado en la LECrim. Las leyes reguladoras de la protección de datos, tanto europeas como nacionales, son las que definen esta categoría, así como los distintos mecanismos de protección con los que cuentan.

El concepto de dato que tiene trascendencia en materia penal es aquél que guarda relación con los hechos objeto de investigación, y que, además, exige ser aportado al proceso. Teniendo esto en consideración, y afectándose alguno de los derechos del art. 18 CE asociados a dichos datos, es necesaria la intervención judicial, la cual permitirá su aportación al proceso.

El contenido de los datos, como objeto de investigación dentro el orden penal es muy amplio, omnicomprensivo y abarca cualquier tipo de dato extraíble de un artefacto electrónico. Lo único que se exige es que el dato que se logre aislar en el equipo informático se relacione con los hechos investigados.

La labor de deslinde de la información de interés para el proceso penal le corresponde al Juez instructor de la causa. Es el Juez el que determinará si debe o no darse traslado a las partes a los efectos de que se pronuncien sobre la existencia o no de cualquier circunstancia que pueda limitar o excluir la incorporación al procedimiento de los datos aparecidos en los aparatos electrónicos.

SEXTA

La LECrim considera los dispositivos de almacenamiento de información de un modo muy amplio, abarcando entre ellos el almacenamiento de información en la nube.

Las diligencias de investigación tecnológica de registro de los datos contenidos en dispositivos de almacenamiento masivo de información y la de acceso a datos mediante el registro remoto de equipos informáticos, tienen por objeto el dato que está dentro de un dispositivo, artefacto o aparato con el que se crea, distribuye, modifica, envía y almacena información.

La LECrim emplea un amplio concepto de dispositivo que incluye a cualquier sistema que permita recoger, almacenar y albergar dichos datos, con independencia de otro de tipo de funcionalidades que pueda tener dicho dispositivo. Esto conlleva que sean considerados como dispositivos de almacenamiento de información tanto un aparato tangible y físico como un dispositivo virtual,

siendo éstos últimos un tipo de servicio ofertado por empresas del sector tecnológico y de las comunicaciones, que permite mediante su empleo guardar los datos y la información que el usuario desee en el interior de un servidor propiedad de la entidad mercantil comercializadora de los mismos.

SÉPTIMA

Las diligencias de acceso y registro de dispositivos electrónicos pueden ser clasificadas de manera autónoma con respecto a las demás diligencias, en concreto pueden ser catalogadas de general a especial.

Las diligencias de investigación tecnológica que permiten el registro de datos contenidos en dispositivos electrónicos se dividen en nuestra legislación en dos tipologías:

1.- Las diligencias de acceso no limitadas a ninguna clase o tipología delictiva determinada. En este caso se trata de una diligencia de carácter estático porque los datos ya se encuentran almacenados en el dispositivo desde que fueron creados por el usuario. Esta diligencia es la regulada en el art. 588 sexies de la LECrim y se corresponde con la de registro de sistemas de almacenamiento masivo de información. Ha de responder para su adopción a los criterios generales de cualquier diligencia que afecte a los derechos del art. 18 CE. Tiene una duración limitada en el tiempo.

2.- Las diligencias de acceso restringido a determinados tipos penales muy graves. Los modos de acceso a datos previsto por la legislación procesal penal para determinados delitos graves resultan más invasivas, en la medida en que se permite que el acceso al dispositivo se realice mediante vías remotas, lo que la convierte en una medida excepcional y de rígidos contornos y presupuestos. Es una diligencia de carácter dinámico, pese a que existan opiniones doctrinales en contra, pues el registro de un equipo en funcionamiento nos da una visión de qué, cómo, cuándo y dónde se está ejecutando alguna actividad en el equipo investigado, lo que es una apreciación directa de la creación, desarrollo, uso e intercambio de los datos investigados.

Es la diligencia regulada en el art. 588 septies de la LECrim y se corresponde con la de registro remoto de equipos informáticos. La adopción de esta diligencia exige la doble concurrencia tanto de los criterios generales de cualquier diligencia que afecte a los derechos del art. 18 CE, como de la observancia de una serie de requisitos específicos. El criterio general de excepcionalidad se extiende en esta diligencia al ámbito temporal, pues su duración es más breve que la diligencia

anterior, como también resulta excepcional la ampliación de los archivos y repositorios a los que se considere necesario extender su práctica.

OCTAVA

El oficio policial debe reunir los argumentos y justificaciones previstos en la ley. La limitación penal de cualquiera de los derechos del art. 18 CE, derivado de la solicitud de la práctica de una diligencia de investigación electrónica, se legitima en la resolución judicial que contenga una minuciosa, detallada, extensa y concreta motivación, exposición y razonamiento de las razones que justifican dicha limitación o afectación del derecho fundamental.

La nueva regulación procesal sobre las diligencias de investigación tecnológica ha reforzado la exigencia de motivación que ha de contener la resolución judicial que acuerda la práctica de la diligencia de registro de dispositivos electrónicos. En la misma línea, también se ha reforzado la exigencia de información que debe suministrar el oficio policial que solicita que se practique alguna de estas nuevas diligencias.

La exigencia de más información en el oficio, y de motivación en la resolución judicial queda justificada por la obligada observancia de la concurrencia de varios principios que ya venían siendo exigidos jurisprudencialmente. De todos estos principios destaca el principio de proporcionalidad, que puede considerarse tanto como un supra principio como un meta principio. Bajo la primera consideración se trata de un criterio que resulta preferente a todos los demás, y que atiende a los propios hechos investigados, a su gravedad y a su trascendencia. Atendiendo a la segunda consideración podemos conceptuarlo como un criterio que abarca a todos los demás. Se trata de la significación y relevancia de los hechos investigados puestos en relación con el derecho que hay que limitar.

NOVENA

La practica de las diligencias de investigación electrónica se caracterizan por la posibilidad de imponer a terceros el cumplimiento de obligaciones generales tanto de conservación de la información alojada en sus dispositivos, como la obligación de su descifrado, decodificación y

entrega a las autoridades. De manera que pueden resultar sancionados, de desobedecer dichas obligaciones, con la apertura de diligencias penales por la comisión de un delito de desobediencia.

Las dos diligencias que constituyen el objeto de esta tesis afectan a los datos electrónicos del investigado, y por ello, ante la necesidad de su obtención, se imponen fuertes obligaciones a terceras personas que puedan auxiliar a los investigadores para que les resulte más seguro y sencillo el acceso a los datos.

La obligación de auxilio que se impone a terceros es más general en la diligencia de acceso al dispositivo, mientras que es mucho más especifica en la diligencia de registro remoto, donde se le dedica un precepto completo. En caso de desatención a esta obligación es posible imputar un delito de desobediencia.

El legislador aclara el concepto de dueño del sistema, dispositivo o sistema de información como sujetos obligados. La doctrina destaca la concurrencia de algunas diferencias con la obligación, de similar naturaleza, recogida también en la regulación de la diligencia de intervención remota de equipos informáticos, defendiéndose, en todo caso, su equiparación. La conclusión que se alcanza es que ambas obligaciones son esencialmente iguales en los dos casos, y se fundamenta esta paridad en que la finalidad pretendida con su establecimiento es la misma en los dos casos: guardar, conservar, asegurar, obtener y desencriptar los datos, y porque la función a desempeñar por estos obligados resulta también idéntica con independencia de la modalidad de registro elegida.

DÉCIMA

Las diligencias de registro de datos realizada tanto de forma directa sobre el dispositivo, como la efectuada de manera remota, no contemplan medidas específicas acerca de la limitación de los derechos del art. 18 CE con respecto a terceras personas.

La nueva regulación procesal sobre las diligencias de investigación empleando medios tecnológicos destaca por su interés y preocupación por salvaguardar los datos de terceras personas ajenos al proceso penal, o bien terceros que estén relacionados con dicho proceso pero que no estén implicados en el mismo. Pese a que en esta materia la legislación se remite a la regulación de cada tipología de diligencia, no se contiene ninguna disposición concreta sobre esta materia, en la

regulación de las diligencias de investigación y registro de dispositivos electrónicos en ninguna de sus dos modalidades.

En la regulación de ambas diligencias hubiera sido deseable que se hubieran establecido algunos criterios específicos que sirvieran para la salvaguarda de estos intereses. En consecuencia, lo que se refiere a la protección de los datos de terceras personas, en los supuestos de las dos diligencias de registro de dispositivos, queda en manos del juez instructor, que será el que pueda disponer de medidas de protección concretas dentro del auto en el que se acuerde su práctica.

UNDÉCIMA

La LECrim regula de manera insuficiente la intervención, acceso y registro de datos contenidos en la nube. Esta específica tipología de registro es vista como un modo de registro adicional o derivado de uno previo.

La actual regulación permite que los datos almacenados en la nube pueden ser registrados durante la investigación penal, empleando para ello las diligencias de los arts. 588 sexies y 588 septies LECrim. La nube se considera por el legislador como un dispositivo más que puede ser objeto de acceso y registro, porque se trata de un tipo de servicio que permite el alojamiento de información que puede resultar de interés para la investigación. El empleo de conceptos como repositorio de datos, parte de un sistema informático o base de datos, son los que permiten concluir con que todo alojamiento virtual se asimila a un dispositivo de almacenamiento de información.

Este tipo de acceso y registro de la información se regula dentro de la diligencia de registro de dispositivos de almacenamiento masivo de información (art. 588 sexies c, apartado 3 de la LECrim), y también en la diligencia de registro remoto de equipos informáticos (art. 588 septies a, apartado 3 de la LECrim).

Las dos tipologías de diligencias admiten el acceso y el registro de los datos almacenados, con independencia del lugar en el que están, aunque sin mencionar en ningún caso la expresión “la nube”. Asimismo ambas modalidades optan por la fórmula de admitir este tipo de registro a dispositivos virtuales partiendo de la ampliación de un registro que haya sido previamente ordenado.

Una primera diferencia entre las dos tipologías de registro se encuentra en que mientras que en el auto que acuerde la medida de registro de dispositivos de almacenamiento de información se puede

permitir desde su adopción, que el acceso a los datos que se contengan en los dispositivos virtuales puedan ser también registrados, ello no es posible en el registro remoto de equipos informáticos, donde cualquier ampliación debe ser objeto de un auto expreso sobre dicho particular.

El tenor literal empleado por el legislador para referirse a algunos de los requisitos que deben concurrir para la admisión de este tipo de registro de dispositivos de almacenamiento de información virtual es confuso. El acceso a la nube se ve limitado a muy concretos casos en los que el acceso a este tipo de dispositivo no necesite, para llegar hasta la información alojada en el mismo, ninguna acción que lo violente o permita llegar a los datos de un modo anómalo o diferente al que lo hace el usuario habitual.

Es defendible la interpretación conforme a la cual se permite el acceso a los datos desde el ordenador o sistema de acceso habitual a dichos datos sin que resulte necesario introducir clave o contraseña porque el usuario así lo tuviera establecido. Es decir, que será valido el acceso si la clave o contraseña no son necesarias, porque de serlo, o bien habrá de solicitarse la autorización del titular o bien habrá de ser un caso en el se pueda realizar este acceso de modo inmediato sin realizar otras operaciones.

La segunda diferencia que se aprecia entre las dos diligencias de registro de datos cuando se refiere al registro de dispositivos virtuales, es el acceso en casos de emergencia. En el registro de dispositivos de almacenamiento masivo de información los investigadores, por razones de urgencia, pueden acceder al contenido de los datos que se albergan en el dispositivo encontrado, y deberán dar cuenta de ellos posteriormente al juez, para que éste ratifique o no dicha actuación, mientras que en el registro remoto de equipos esto no es posible, debiéndose dar cuenta al juez del hecho, y solicitar nuevo acceso remoto.

En una regulación tan reciente como la relativa a las diligencias que afectan a los derechos del art. 18 CE, hubiera sido deseable una mayor claridad en la regulación del acceso a los datos albergados en la nube. Esta transparencia se hace necesaria en lo que se refiere al modo de acceder a los datos, así como también respecto de aspectos derivados, como, por ejemplo, la limitación de la jurisdicción del Juez instructor en los casos en los que se desconoce el paradero de la información virtual.

DUODÉCIMA

La LECrim no tiene en cuenta que la ubicación de los datos alojados en la nube puede afectar a la jurisdicción del Juez español, en la medida en que ésta no alcanza para ejecutar el

registro de la información alojada en la nube cuando no se puede acceder a ella desde el dispositivo y la misma puede estar fuera del territorio nacional. La redacción legal sobre este aspecto resulta insuficiente, y no hay mención al proceso a seguir cuando la información no sea accesible, lo que ha abierto varias posturas en la doctrina tendentes a justificar desde la existencia de dicha jurisdicción en el Juez de Instrucción hasta la inexistencia de la misma.

La intangibilidad de los datos informáticos y la capacidad para alojarse en servidores de cualquier lugar ha sido una cuestión completamente obviada por la legislación internacional que sigue muy apegada al componente territorial como elemento determinante para acceder y registrar los servidores en los que los datos están alojados, como también de la legislación aplicable en orden a su protección.

El legislador español permite que los datos alojados en la nube puedan ser registrados mediante una orden dictada por el juez nacional, con independencia de su ubicación territorial. Esta posibilidad solo resulta viable cuando la facilidad de acceso a los datos se traduce en la innecesariedad de operar con el ordenador para que se permita este acceso, bien sea porque es conocida la clave o contraseña de acceso, bien porque la simple puesta en marcha del dispositivo admite el acceso al dispositivo virtual. Pero fuera de estos supuestos, que tampoco resultan muy claros en el texto legal, la Ley no niega la posibilidad de realizar estos registros, lo que pone en entredicho la facultad de la jurisdicción española para realizar este tipo de diligencias cuando los datos se encuentran fuera del territorio nacional.

Ante esta indefinición se han desarrollado diferentes posiciones dentro la doctrina científica en la que se tratan de justificar las diversas opciones posibles, desde considerar que el Juez español tiene jurisdicción para el registro virtual, a considerar que la tiene sólo en algunos casos, o hasta rechazar la concurrencia de dicha jurisdicción y la necesidad de acudir a los mecanismos de cooperación judicial que resulten necesarios en aras a no comprometer la validez de la diligencia, a costa de perder rapidez en la investigación.

DÉCIMO TERCERA

La imposibilidad de acceso a los datos alojados en la nube por los medios previstos expresamente en la LECrim exige acudir a las vías de cooperación judicial internacional, o bien solicitar estos datos a las empresas que las alojan, como fórmulas de acceso que eviten exponer todo o parte del proceso a nulidad por vulneración de derechos fundamentales.

Los datos que se encuentran alojados en la nube pueden encontrarse almacenos en los servidores de las empresas que ofrecen este tipo de servicios. Estos servidores pueden encontrarse fuera del territorio nacional, lo que puede conllevar una falta de jurisdicción del Juez instructor en el momento de ordenar el acceso y registro directo de los mismos. El Juez español requiere auxilio y la cooperación de otros órganos judiciales extranjeros para actuar fuera del territorio nacional.

Es necesario que en los casos en que los datos puedan estar ubicados fuera de las fronteras españolas, el oficio policial que insta al registro de dispositivo virtual ponga de manifiesto cuál es el territorio en el que se encuentra el repositorio que aloja dicha información, o bien si no lo hace, el juez instructor solicite a los investigadores, por vía del complemento del oficio, un informe sobre la ubicación real de los datos. De esta forma se contará con la información suficiente para que el auto que acuerde la diligencia de acceso y registro a un dispositivo virtual determine lo más adecuado, evitándose el dictado de una resolución con tal desconocimiento, lo que comportará claras consecuencias procesales sobre su validez.

En el caso en que el dispositivo electrónico desde el que se produce el acceso a los datos virtuales necesite una manipulación en el mismo o exija recabar el usuario o la contraseña y ésta no se preste voluntariamente, será necesario acudir a vías distintas para obtener la información. Una posibilidad frecuente es ordenar a las compañías que prestan el servicio de alojamiento de información que aporten estos datos, o bien, si se trata de realizar un registro, usar fórmulas de cooperación judicial internacional, si se conoce donde están alojados los datos o se tiene conciencia de que su paradero está fuera del territorio nacional.

Esta conclusión está avalada por la regulación que ofrece el Convenio sobre Ciberdelincuencia, que exige la presencia de los datos en el territorio nacional para ordenar la intervención de los datos necesarios para la investigación.

No está habilitado, ni autorizado ninguna clase de acceso al ordenador usando manipulaciones informáticas posibilitadas por el estado de la técnica, salvo en los concretos casos previstos para realizar la diligencia de acceso remoto a equipos informáticos. En esta diligencia concreta, el acceso a los datos alojados en una nube queda a la valoración judicial, sin que en su concreta regulación se haga alusión a ningún modo de acceso como en el caso de la diligencia de registro de dispositivo de almacenamiento masivo.

Es ante la indefinición legal, por lo que se recomienda acudir a los mecanismos de cooperación judicial internacional para que se puedan recabar los datos necesarios para la investigación. La obtención de los datos mediante los mecanismos de cooperación judicial usando los medios de

auxilio previstos en leyes y tratados evitan declaraciones de nulidad de actuaciones principales y de las derivadas, pero como contrapartida, ralentizan la investigación.

Existen variados mecanismos de cooperación judicial internacional, algunos propios de la UE, que permiten al juez nacional acudir a ellos en los casos en los que no pueda realizar una determinada diligencia de investigación o existan dudas de legalidad sobre ello. Estos mecanismos consisten en medidas legislativas tendentes a coordinar diferentes autoridades judiciales nacionales para que unas puedan llevar a cabo las medidas de investigación ordenadas por otras; la creación de organizaciones dedicadas a la coordinación y el enlace entre diversas autoridades judiciales nacionales, y la creación, desarrollo y aplicación de distintas herramientas tanto de coordinación efectiva, como de naturaleza informática, encaminadas al auxilio y consulta.

DÉCIMO CUARTA

La información obtenida por la practica de un registro de datos contenidos en sistemas y dispositivos informáticos se considera como una prueba preconstituída, y está sujeta a contradicción mediante la practica de otras diligencias de investigación y otras pruebas.

El resultado de las diligencias de investigación de acceso a dispositivos de almacenamiento masivo de información, o las obtenidas mediante el acceso remoto a equipos, constituyen una prueba preconstituida. El contenido del resultado de la práctica de estas diligencias se incorpora a las actuaciones penales será mediante la aportación de los datos encontrados en el dispositivo, así como a través del informe pericial entregado por los investigadores al Juez instructor.

El resultado de las diligencias puede refutarse por cualquier otra diligencia realizada a instancias de las partes tendentes a su ratificación, o bien a su impugnación. La aportación de un informe pericial será la forma más adecuada para reflejar el resultado obtenido del registro de datos y que resulte comprensible para el juzgador y las partes.

En todo caso los medios de prueba previstos en derecho como son la documental, testifical, examen judicial, no quedan excluidos en ningún caso como medio de contradicción. El auto puede concretar algún aspecto sobre el modo en que los datos deben ser aportados por los investigadores a las actuaciones para mejorar la comprensión del resultado y el acceso de las partes.

DÉCIMO QUINTA

El resultado de las diligencias de investigación electrónica puede ser impugnado mediante el empleo de cualquiera de los recursos previstos en derecho, siendo una de las causas que más se emplea para impugnar su resultado la existencia de algún vicio de nulidad.

La resolución que acuerde la realización de una diligencia de registro remoto a un equipo informático o a un dispositivo de almacenamiento masivo puede someterse a cualquiera de los mecanismos de impugnación existentes en la legislación procesal.

Las impugnaciones pueden dirigirse contra la decisión de adopción o denegación de la práctica de la diligencia, lo que deberá hacerse valer mediante la interposición, en tiempo y forma legal, de los recursos de reforma o de apelación oportunos. Asimismo, se podrá alegar que la practica de la misma, y la resolución que la acuerda pueda adolecer de algún defecto que la invalide, por haberse acordado, practicado o incorporado al proceso con vulneración de derechos fundamentales, lo que convierte a la nulidad en uno de los motivos más empleados en estos casos.

DÉCIMO SEXTA

Las diligencias de investigación electrónica practicadas en la fase de instrucción se convierten en un medio de prueba, una vez que acceden al proceso y llegan a la fase de enjuiciamiento. Por ello resultan susceptibles de ser valoradas por el juez decisor con plena libertad de criterio, sin que su naturaleza electrónica implique o exija mayores requisitos en orden a la valoración.

Las diligencias de investigación realizadas durante la instrucción tienen por finalidad el ser objeto de valoración por parte del Juez encargado de entrar a conocer sobre el fondo del asunto.

El resultado que aportan las diligencias de acceso y registro de dispositivos que alojan información entra en la categoría denominada por la doctrina como prueba tecnológica, que tiene un mayor desarrollo en el ámbito del proceso civil. En todo caso, en el ámbito del proceso penal, la valoración de esta prueba, por parte del juez o tribunal encargado del enjuiciamiento, está sometida a la lógica y a la conciencia.

8. RESOLUCIONES JUDICIALES CITADAS

Tribunal de justicia de la Unión Europea.

STJUE (Gran Sala) de 21 de diciembre de 2016.

STJUE (Gran Sala) de 2 de octubre de 2018. Asunto C-207/16.

Tribunal Europeo de Derechos Humanos.

Decisión del Tribunal Europeo de Derechos Humanos (Sección 4ª) de 15 diciembre 1998. Caso A.E.D.L.G contra España.

Decisión del Tribunal Europeo de Derechos Humanos (Sección 4ª), de 18 de octubre de 2005, Caso Roldán Ibáñez contra España.

Decisión del 7 de septiembre de 2010 Tribunal Europeo de Derechos Humanos (Sección 3ª). Caso Fernández Saavedra contra España.

STEDH (Sección 1ª), de 26 marzo 2015, Caso Volkov y Adamskiy contra Rusia.

STEDH (Sección 3ª), de 11 octubre 2016, Caso Iglesias Casarrubios y Cantalapiedra Iglesias contra España.

STEDH (Sección 3ª), de 30 de mayo de 2017, Caso Trabajo Rueda contra España.

Tribunal Constitucional

STC 19/1981, de 8 de junio. Ponente: Don Ángel Latorre Segura

STC 25/1981, de 14 de julio. Ponente: Don Antonio Truyol Serra.

STC 31/1981, de 28 de Julio. Ponente: Doña Gloria Begue Cantón.

STC 31/1983 de 27 de abril. Ponente: Don Antonio Truyol Serra.

STC 22/1984, de 17 de febrero. Ponente: Don Luis Díez-Picazo y Ponce de León.

STC 181/1984, de 20 de junio. Ponente: Don Rafael de Mendizábal Allende.

STC 114/1984, de 29 de noviembre. Ponente: Don Luis Díez-Picazo y Ponce de León.

STC 53/1985, de 11 de abril. Ponentes: Doña Gloria Begué Cantón y Don Rafael Gómez Ferrer Morant.

STC 126/1986 de 22 de octubre. Ponente: Don Francisco Rubio Llorente.

STC 37/1989, de 15 de febrero. Ponente: Don Francisco Rubio Llorente

STC 46/1990, de 15 de marzo. Ponente: Don Vicente Gimeno Sendra.

STC 223/1992, de 14 de diciembre. Ponente: Don Rafael de Mendizábal Allende.

STC 86/1995, de 6 de junio. Ponente: Don Vicente Gimeno Sendra.

STC 49/1996 de 26 de marzo. Ponente: Don Manuel Pérez de Parga y Cabrera.

STC 188/1998 de 28 de septiembre. Ponente: Don Fernando García-Mon y González Regueral

STC 43/2000, de 14 de febrero. Ponente: Doña María Emilia Casas Bahamonde.

STC 126/2000, de 16 de mayo. Ponente: Don Vicente Conde Martín de Hijas.

STC 202/2001, de 15 de octubre. Ponente: Don Guillermo Jiménez Sánchez.

STC 10/2002, de 17 de enero. Ponente: Doña Emilia María Casas Bahamonde.

STC 17/2002 de 28 enero. Ponente: Doña Elisa Pérez Vera.

STC 70/2002, de 3 de abril, Ponente: Don Fernando Garrido Falla,

STC 82/2002, de 22 de abril. Ponente: Doña María Emilia Casas Bahamonde.

STC 120/2002, de 20 de mayo Ponente: Don Fernando Garrido Falla.

STC 123/2002, de 20 de mayo. Ponente: Doña María Emilia Casas Bahamonde.

STC 167/2002 de 18 septiembre. Ponente: Don Vicente Conde Martín de Hijas.

STC 25/2003 de 10 de febrero, Ponente: Doña Elisa Pérez Vera.

STC 56/2003, de 24 de marzo. Ponente: Doña Elisa Pérez Vera.

STC 93/2005, de 18 de abril. Ponente: Don Roberto García Calvo y Montiel.

STC 233/2005, de 26 de septiembre de 2005. Ponente: Don Guillermo Jiménez Sánchez.

STC 104/2006, de 3 de abril. Ponente: Doña Emilia Casas Bahamonde.

STC 156/2007, de 2 de julio. Ponente: Don Javier Delgado Barrio.

STC 230/2007, de 5 de noviembre, ponente: Doña María Emilia Casas Bahamonde.

STC 184/2009, de 7 de septiembre. Ponente: Doña Elisa Pérez Vera.

STC 30/2010, de 17 de mayo. Ponente**:** Doña Elisa Pérez Vera

STC 68/2010 de 18 octubre, ponente Doña Elisa Pérez Vera

STC 72/2010, de 18 de octubre. Ponente: Don Eugenio Gay Montalvo.

STC 173/2011, de 7 de noviembre. Ponente: Don Eugenio Gay Montalvo.

STC 29/2013, de 11 de febrero. Ponente: Don Fernando Valdés Dal-Ré.

STC 115/2013, de 9 de mayo. Ponente: Don Manuel Aragón Reyes.

STC 208/2013, de16 de diciembre. Ponente: Doña Adela Asua Batarrita.

STC 145/2014, de 22 de septiembre. Ponente: Don Fernando Valdés Dal-Ré

STC 65/2015, de 3 de abril, Ponente: Don Francisco Pérez de los Cobos Orihuel.

STC 18/2015, de 16 de febrero. Ponente: Don Pedro José González-Trevijano Sánchez.

STC 77/2016, de 25 de abril. Ponente: Don Pedro González-Trevijano Sánchez.

STC 21/2018, de 5 de marzo de 2018. Ponente: Don Cándido Conde-Pumpido Tourón.

Tribunal Supremo

STS 2054/1993, de 10 de junio de 1993. Ponente: D. Enrique Ruíz Vadillo.

STS 2324/1993, de 24 de junio de 1993. Ponente: D. Enrique Ruíz Vadillo.

STS 721/1996, de 18 de octubre. Ponente: Don Cándido Conde Pumpido Tourón.

STS 1947/2002, de 29 de diciembre. Ponente: D. Joaquín Jiménez García.

STS 446/2004, de 19 de enero de 2005. Ponente: Don Andrés Martínez Arrieta.

STS. 814/2006 de 14 julio. Ponente: D. Joaquín Delgado García.

STS 901/2006 de 27 de septiembre. Ponente: Don Juan Ramón Berdugo y Gómez de la Torre

STS 71/2007, 8 de febrero. Ponente: Don Juan Ramón Berdugo y Gómez de la Torre.

STS 358/2007, de 30 de abril. Ponente: Don Miguel Colmenero Menéndez de Luarca.

STS 487/2007, de 29 de mayo. Ponente: Manuel Marchena Gómez.

STS 642/2007, de 6 de julio. Ponente: Don Manuel Marchena Gómez.

STS 233/2008, de 5 de mayo. Ponente: Don Manuel Marchena Gómez.

STS 256/2008, de 14 de mayo. Ponente: Don Perfecto Andrés Ibáñez

STS 249/2008, de 20 de mayo. Ponente: Don Manuel Marchena Gómez.

STS 151/2009, de 11 de febrero. Ponente: Don Adolfo Prego de Oliver y Tolivar.

STS 691/2009, de 5 de junio. Ponente: Don Adolfo Prego de Oliver y Tolivar.

STS 737/2009 de 6 de julio. Ponente: Don Joaquín Jiménez García.

STS 1119/2009, de 6 de noviembre. Ponente: Don Alberto Gumersindo Jorge Barreiro.

STS 1140/2010 de 29 de diciembre. Ponente: Don Juan Ramón Berdugo y Gómez de la Torre.

STS 53/2011, de 10 de febrero de 2011. Ponente: Don Juan Ramón Berdugo y Gómez de la Torre.

STS 64/2011, de 8 de febrero, Ponente: Don Francisco Monterde Ferrer.

STS 1045/2011, de 14 de octubre. Ponente: Don Juan Ramón Berdugo y Gómez de la Torre.

STS 79/2012, de 9 de febrero. Ponente: Don Miguel Colmenero Menéndez de Luarca.

STS 79/2012, de 9 de febrero. Ponente: Don Andrés Martínez Arrieta.

STS 60/2012, 8 de febrero. Ponente: Don Juan Ramón Berdugo y Gómez de la Torre.

STS 751/2012, de 28 de septiembre. Ponente: Don Manuel Marchena Gómez.

STS 722/2012, de 2 de octubre. Ponente: D. Cándido Conde Pumpido-Tourón.

STS 342/2013, de 17 de abril. Ponente: Don Manuel Marchena Gómez.

STS 950/2013, de 5 de diciembre, Ponente: Don Julián Artemio Sánchez Melgar.

STS 1008/2013, de 8 de enero de 2014. Ponente: Don Cándido Conde-Pumpido Tourón.

STS 513/2014, de 24 de junio. Ponente: Juan Ramón Berdugo y Gómez de la Torre.

STS, 759/2014, de 25 de noviembre de 2014. Ponente: Don Juan Ramón Berdugo y Gómez de la Torre.

STS 789/2014, de 2 de diciembre. Ponente: Don Juan Ramón Berdugo y Gómez de la Torre.

STS 807/2014, de 2 de diciembre de 2014. Ponente: Don Miguel Colmenero Menéndez de Luarca.

STS 97/2015, de 24 de febrero. Ponente: Don Juan Ramón Berdugo y Gómez de la Torre.

STS 203/2015, de 23 de marzo. Ponente: Don Julián Artemio Sánchez Melgar.

STS 176/2015, de 25 de marzo. Ponente: Don Francisco Monterde Ferrer.

STS 187/2015, de 14 de abril. Ponente: Don Francisco Monterde Ferrer.

STS 292/2015, de 14 de mayo. Ponente: Don Joaquín Jiménez García.

STS 393/2015, de 12 de junio. Ponente: D. Juan Maza Martín.

STS 468/2015, de 16 de julio. Ponente: Don Andrés Palomo del Arco.

STS 545/2015, de 15 de octubre. Ponente: Don Rafael Sarazá Jimena.

STS 754/2015, de 27 de noviembre. Ponente: Don Julián Artemio Sánchez Melgar.

STS 786/2015, de 4 de diciembre. Ponente: Don Manuel Marchena Gómez.

STS 982/2016, de 11 de enero de 2017 Ponente: Don Joaquín Jiménez García.

STS 154/2016 de 29 de febrero de 2016. Ponente: Don José Manuel Maza Martín.

STS 165/2016, de 2 de marzo. Ponente: Don Alberto Jorge Barreiro

STS 204/2016, de 10 de marzo. Ponente: Don Cándido Conde Pumpido-Tourón.

STS 841/2016, de 8 de noviembre. Ponente: Don Juan Ramón Berdugo y Gómez De la Torre.

STS 878/2016, 22 de noviembre. Ponente: Don Andrés Palomo del Arco.

STS 972/2016, de 21 de diciembre. Ponente: Don Andrés Palomo del Arco.

STS 991/2016, de 12 de enero de 2017. Ponente: Don Alberto Gumersindo Jorge Barreiro.

STS 993/2016, de 12 de enero de 2017. Ponente: Don Joaquín Jiménez García

STS 160/2016 de 1 de marzo, Ponente: Don Manuel Marchena Gómez

STS 167/2016, de 2 de marzo. Ponente: Don Juan Saavedra Ruíz.

STS 210/2016, de 5 de abril de 2016. Ponente: Don Rafael Sarazá Jimena.

STS 689/2016 de 27 de julio. Ponente: Don Pablo Llarena Conde.

STS 85/2017, de 15 de febrero. Ponente: Don Joaquín Jiménez García.

STS 106/2017, de 21 de febrero. Ponente: Don Antonio del Moral.

STS 116/2017, de 23 de febrero. Ponente: D. Manuel Marchena Gómez.

STS 196/2017, de 24 de marzo. Ponente: Don Carlos Granados Pérez.

STS 213/2017, de 29 de marzo. Ponente: Don Carlos Granados Pérez.

STS 200/2017, de 27 de marzo. Ponente: Don Juan Ramón Berdugo Gómez de la Torre.

STS 271/2017, de 18 de abril. Ponente: Doña Ana María Ferrer García.

STS 272/2017, de 18 de abril. Ponente: Don Juan Saavedra Ruíz.

STS 287/2017, de 19 de abril. Ponente: Don Manuel Marchena Gómez.

STS 358/2017, de 18 de mayo. Ponente: Don Carlos Granados Pérez.

STS 400/2017, de 1 de junio. Ponente: Don Juan Saavedra Ruíz

STS 508/2017, de 4 de julio. Ponente: Don Manuel Marchena Gómez.

STS 426/2017, de 6 de julio Ponente: Don Rafael Sarazá Jimena.

STS 546/2017, de 12 de julio. Ponente: Don Luciano Varela Castro.

STS 446/2017, de 13 de julio. Ponente: Don Rafael Sarazá Jimena.

STS 556/2017, de 13 de julio. Ponente: D. José Ramón Soriano Soriano.

STS 641/2017, de 28 de septiembre. Ponente: Don Juan Ramón Berdugo Gómez de la Torre.

STS 645/2017, de 2 de octubre. Ponente: Don Juan Ramón Berdugo Gómez de la Torre

STS 661/2017 de 10 de octubre. Ponente: Don Alberto Jorge Barreiro.

STS 703/2017, de 25 de octubre. Ponente: Don Andrés Martínez Arrieta.

STS 119/2018, de 8 de febrero. Ponente: D. Luis Fernando de Castro Fernández.

STS 47/2018, de 17 de enero. Ponente: D. Nicolás Maurandi Guillen.

STS 228/2018, de 17 de mayo. Ponente: Doña Ana María Ferrer García.

STS 216/2018, de 8 de mayo. Ponente: don Vicente Magro Servet.

STS 489/2018, de 23 de octubre de 2018. Pte: Don Antonio del Moral García

STS 723/2018, de 23 de enero de 2019. Ponente: Doña Ana María Ferrer García.

STS 462/2019, de 14 de octubre de 2019. Ponente: D. Pablo Llarena Conde.

Auto del TS de 28 febrero 2018. Ponente: D. Andrés Martínez Arrieta

Audiencia Nacional

SAN 25/2016, de 28 de septiembre. Ponente: Don Fermín Javier Echarri Casi.

SAN 6/2017, de 10 de marzo. Ponente: Don Fermín Javier Echarri Casi.

SAN en recurso 190/2016, de 21 de octubre de 2017, Ponente: Doña Felisa Atienza Rodríguez.

Tribunales Superiores de Justicia

Auto del TSJ Madrid 50/2017, de 16 de mayo. Ponente: Don Francisco Javier Vieira Morente.

Audiencias Provinciales

SAP de Madrid 1235/2002, de 27 de junio. Ponente: Don José Antonio Ramos Gancedo.

SAP de Pontevedra 5/2006, de 10 de mayo. Ponente: D. Manuel Almenar Belenguer.

SAP de Madrid 154/2007, de 9 de abril. Ponente: Doña Araceli Perdices López.

SAP de Barcelona 288/2016, de 12 de junio. Ponente: Don José Grau Gasso.

SAP de Guadalajara 24/2017, de 17 de enero. Ponente Dña. María Victoria Hernández Hernández.

SAP de Cáceres, Sección 2º, 12/2017, de 25 de enero. Ponente: Don Jesús María Gómez Flores.

SAP de Cádiz, Sección 1º, 335/2017 de 29 de diciembre. Ponente: Don Francisco Javier Gracia Sanz.

SAP de Bilbao 90097/2017, de 12 de abril. Ponente: Doña Elisa Pisonero del Pozo Riesgo.

SAP de Jaén 553/2017 de 3 de septiembre. Ponente: Doña María Fernanda García Pérez.

SAP de Madrid, sección 30, 316/2018, de 3 de mayo. Ponente: Doña Inmaculada López Candela.

SAP de Zaragoza, sección 6º, 164/2018, de 12 de junio. Ponente: Don Rubén Blasco Obede.

SAP de Cartagena, sección 5ª, 39/2019, de 12 de febrero de 2019. Ponente: Don José Manuel Nicolás Manzanares.

Auto de la Audiencia Provincial de Tarragona (Sección 4º) 6 de abril de 2016. Ponente: Don Javier Hernández García.

Auto de la Audiencia Provincial de Barcelona 214/2017, de 1 de marzo. Ponente: Doña Elena Guindulaín Oliveiras.

Auto de la Audiencia Provincial de Barcelona 215/2017, de 1 de marzo. Ponente: Doña Elena Guindulaín Oliveiras.

Auto de la Audiencia Provincial de Pontevedra 223/2017, de 21 de marzo. Ponente: Don José Juan Ramón Barreiro Prado.

Auto de la Audiencia Provincial de Lugo 315/2017, de 28 de marzo. Ponente: Doña Ana Rosa Pérez Quintana.

Auto de la Audiencia Provincial de Soria 167/2017, de 26 de septiembre. Ponente: Doña Belén Pérez-Flecha Díaz.

Auto de la Audiencia Provincial de Murcia (sección 3º) 939/2017 de 27 octubre. Ponente: Doña Ana María Martínez Blázquez

Auto de la Audiencia Provincial de Pontevedra (Sección 5ª) 794/2017 de 9 noviembre. Ponente: Dña. María Belén Rubido de la Torre.

Auto de la Audiencia Provincial de Tarragona 615/2017, de 24 de noviembre. Ponente: Don Francisco José revuelta Muñoz.

Auto de la Audiencia Provincial de Álava, sección segunda, 255/2018, de 9 de mayo. Ponente: Doña Ana Jesús Zulueta Álvarez.

9. BIBLIOGRAFIA.

AGENCIA ESPAÑOLA DE PROTECCION DE DATOS, *Guía para clientes que contraten servicios de Cloud Computing*. Madrid. 2013.

ALAMILLO DOMINGO, Ignacio. «El control de localización de los datos e informaciones en el Cloud» en MARTÍNEZ MARTÍNEZ RICARD (Editor), *Derecho y Cloud Computing.* Thomson Reuters- Aranzadi. Pamplona. 2012.

ALBALADEJO, Manuel. *Derecho Civil I. Introducción y parte general*. EDISOFER. Madrid. 2013

ÁLVAREZ CONDE, Enrique y TUR AUSINA, Rosario. *Derecho constitucional*. sexta edición. Madrid. Tecnos. 2016.

ÁLVAREZ CONDE, Enrique. *Curso de Derecho constitucional*. sexta edición. Madrid. Tecnos. 2008

ÁLVAREZ DE NEYRA KAPPLER, Susana. «Los descubrimientos casuales en el marco de una investigación penal (con especial referencia a las diligencias de entrada y registro en domicilio». *Revista internacional de Estudios de derecho procesal y arbitraje*. Septiembre de 2011.

ÁLVAREZ SÁNCHEZ DE MOVELLÁN, Pedro. *El incidente de nulidad de actuaciones: solución o problema frente a la resolución firme.* Madrid. Dykinson. 2015.

ALZAGA VILLAAMIL, Oscar, GUTIÉRREZ GUTIÉRREZ, Ignacio y RODRÍGUEZ ZAPATA, Jorge. *Derecho Político español, según la Constitución de 1978. II. Derechos fundamentales y órganos del Estado*. Tercera Edición. Editorial Centro de Estudios Ramón Areces. SA. Madrid. 2002.

APARICIO VAQUERO, Juan Pablo. «La protección de datos que viene: el nuevo Reglamento General europeo. The forthcoming data protection: the new European General Regulation». *Ars Iuris Salmanticensis Tribuna de Actualidad* Vol. 4, 27-34 diciembre 2016.

AREITIO RODRIGO, Ramón. *Lecciones elementales de Derecho Natural*. Publicaciones de la Universidad de Deusto, 1996.

ARENAS, Guillermo. «¿Donde se guarda lo que subes a la nube?». *EL PAIS. Sección Tendencias. Perteneciente a la revista RETINA*. Edición digital 11 de enero de 2018.

ARMENTA DEU, Teresa. «La reforma del recurso de Apelación y la generalización de la segunda instancia». *JUSTICIA: Revista de Derecho procesal.* Núm.: 1/2016. enero de 2016.

ARRABAL PLATERO, Paloma. *La prueba tecnológica: aportación, práctica y valoración*. Tirant lo Blanch. Valencia. 2020.

AZAUSTRE RUÍZ, Pablo. «Acercamiento al régimen jurídico procesal previsto para la utilización de la información obtenida en un procedimiento penal distinto» en COLOMER HERNÁNDEZ, Ignacio. (Dir) *Cesión de datos personales y evidencias entre procesos penales y procedimientos administrativos sancionadores o tributarios*. Thomson Reuters Aranzadi. Pamplona 2017.

BACHMAIER WINTER, Lorena. «Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015». *Boletín del Ministerio de Justicia*. Número 2195. Enero 2017. ISSN: 1989-4767 NIPO: 051-15-001-5.

BALLESTEROS MOFFA, Luís Ángel. «La difícil situación de la Ley 25/2007 de conservación y cesión de datos de tráfico y localización en las comunicaciones electrónicas: la «tala» de su base comunitaria y los desfavorables vientos desde sus homólogas europeas». *Revista Aranzadi de Derecho y Nuevas Tecnologías* núm. 44/2017 parte Estudios jurídicos. BIB 2017\12592.

BONILLA CORREA, Jesús Ángel «Los avances tecnológicos y sus incidencias en la ejecución de la diligencia de registro en domicilio (1)». *Diario La Ley*, Nº 8522, 20 de abril de 2015. LA LEY 2772/2015 I.

BUENO DE MATA, Federico. «Comentarios y reflexiones sobre la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica». Diario La Ley, Nº 8627, 19 de octubre de 2015, LA LEY 5958/2015.

BUENO DE MATA, Federico «Comentarios críticos y reflexiones acerca de las últimas reformas procesales en materia de investigación tecnológica» en RODRÍGUEZ TIRADO, Ana María (Coord). *Cuestiones actuales de Derecho Procesal*. Tirant Lo Blanch. Valencia. 2017.

BUENO DE MATA, Federico. *Las diligencias de investigación penal en la cuarta revolución industrial. Principios teóricos y problemas prácticos*. Aranzadi. Navarra. 2019.

BUENO GALLARDE, Esther. *La configuración constitucional del derecho a la intimidad. En particular el derecho a la intimidad de los obligados tributarios*. Centro de Estudios Políticos y Constitucionales. Madrid. 2009

CABEZUDO BAJO, María José. *La inviolabilidad del domicilio y el proceso penal.* Iustel. Madrid. 2004.

CANO PAÑOS, Miguel Ángel. «Los delitos de terrorismo en el Código penal español tras a reforma de 2010». *La Ley Penal*, Nº 86, octubre 2011. LA LEY 16987/2011.

CASANOVA MARTÍ, Roser. *Las intervenciones telefónicas en el proceso penal*. J&B BOSCH PROCESAL. España. 2014.

CAVERO FORRADELLAS, Gerardo. «*La nueva regulación de las intervenciones telefónicas en la Ley de enjuiciamiento criminal»*. Ponencias de formación de fecha 27 de abril de 2016, Jornadas denominadas "La interceptación de las comunicaciones telefónicas y telemáticas". Enlace: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20Cavero%20Forradellas,%20Gerardo.pdf?idFile=38380825-2079-4304-af21-40d9010e0ae9

COLOMER HERNÁNDEZ, Ignacio. *La motivación de las sentencias: sus exigencias constitucionales y legales.* Tirant lo Blanch. Valencia. 2003.

COLOMER HERNÁNDEZ, Ignacio (Dir). *Cesión de datos personales y evidencias entre procesos penales y procedimientos administrativos sancionadores y tributarios*. Aranzadi. Pamplona. 2017.

COLOMER HERNÁNDEZ, Ignacio «Uso y cesión de datos de las comunicaciones electrónicas para investigar delitos tras la STJUE de 21 de diciembre de 2016», en RUDA GONZÁLEZ, Albert (Coord.) y JEREZ DELGADO, Carmen (Coord), *Estudios sobre Jurisprudencia Europea.*

Materiales del I y II encuentro anual del Centro español del European Law Institute. Ed. Sepin. Madrid. 2018.

COLOMER HERNÁNDEZ, Ignacio, «La prueba tecnológica», en GONZÁLEZ CANO, María Isabel (Dir), *La Prueba. Tomo I. La Prueba en el Proceso civil*. Tirant lo Blanch. Valencia. 2017.

CONDE PUMPIDO TOURÓN, Cándido. «*La reforma procesal. Registro de sistemas informáticos, ampliación del registro a otros sistemas. El registro remoto de dispositivos informáticos (arts. 588 sexies y 588 septies LECRIM)»*. Ponencia presentada en las Jornadas de formación organizadas por la Fiscalía General del Estado con fecha 10 de marzo de 2016 en materia de criminalidad informática. Enlace: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20Conde-Pumpido%20Tourón.pdf?idFile=4d9fe168-e9ee-4cd9-a783-68eab6158e47

CUADRADO SALINAS, Carmen. «Registro informático y prueba digital. Estudio y análisis comparado de la ciberinvestigación criminal en Europa (1)». *La Ley Penal,* Nº 107, Sección Estudios, Marzo-Abril 2014, Editorial Wolters Kluwer. LA LEY 1257/2014.

CUCARELLA GALIANA. Luis-Andrés. «Autorización judicial de registro remoto de equipos informáticos». *Revista General de Derecho Procesal*, nº 38. (año 2016).

CUESTA, José Luis. «Cloud, una oportunidad para la Administración Pública». *Estrategia Financiera*, Nº 292, 28 de febrero de 2012. LA LEY 2017/2012.

DAVARA RODRÍGUEZ, Miguel Ángel «DEBE CONOCER: Consulta pública de la Agencia Española de Protección de Datos sobre computación en nube». *El Consultor de los Ayuntamientos*, Nº 3, Quincena del 15 al 29 Feb. 2012, Ref. 359/2012, tomo 1, Editorial Wolters Kluwer.

DAVARA RODRÍGUEZ, Miguel Ángel. *Manual de derecho informático*. 11a ed. (rev. y puesta al día). Cizur Menor Aranzadi. 2015.

DELGADO MARTÍN, Joaquín. «La prueba electrónica en el proceso penal». *Diario La Ley*, Nº 8167, 10 de octubre de 2013. LA LEY 7336/2013.

DELGADO MARTÍN, Joaquín. *La investigación tecnológica y la prueba digital en todas las jurisdicciones*. Wolter Kluwer. Madrid. 2016.

DELGADO MARTÍN, Joaquín. «Investigación del entorno virtual: el registro de dispositivos digitales tras la reforma por LO 13/2015». *Diario La Ley*, Nº 8693, 2 de febrero de 2016. LA LEY 229/2016.

DELGADO MARTÍN, Joaquín. «La prueba digital concepto clases, aportación al proceso y su valoración». *Diario La Ley*, Nº 6, 11 de abril de 2017. LA LEY 3841/2017 I.

DÍEZ-PICAZO JIMÉNEZ, I. «El derecho fundamental al juez predeterminado por la ley». *Revista Española de Derecho constitucional*. Año 11, nº 31. Enero – abril 1991.

DORESTE ARMAS, Delia Carolina. «El espacio judicial europeo y la fiscalía europea como órgano de investigación y persecución penal; versus modelo procesal español. European area of justice and european public prosecutor as responsible for investigating and prosecuting; versus spanish criminal process». *Diario La Ley*, Nº 8981, 17 de Mayo de 2017.

ECHARRI CASI, Fermín Javier. «Prueba ilícita: conexión de antijuridicidad y hallazgos casuales» *Revista del Poder Judicial* nº 69, 2003.

EIRANOVA ENCINAS, Emilio. *Código penal alemán, StGB Código Procesal Penal alemán StPO*. Marcial Pons. Madrid. 2000.

FERNÁNDEZ GALIANO, Antonio y DE CASTRO CID, Benito. *Lecciones de Teoría del Derecho y Derecho Natural*. Editorial Universitas, SA. Madrid. 2001.

GARCÍA PÉREZ, Rafael. «Los desafíos de la Unión Europea en la gobernanza global». *Cuadernos Europeos Deusto*. Núm. 45/2011.

GARCÍA SAN MARTÍN, Jerónimo. «El hallazgo casual o descubrimiento ocasional en el ámbito de la investigación penal». *La Ley Penal*, Nº 109, Julio-Agosto 2014. LA LEY 4917/2014.

GARCÍA SAN MARTÍN, Jerónimo. «Consideraciones en torno al anteproyecto de Ley Orgánica de modificación de la Ley de Enjuiciamiento Criminal para la agilización de la justicia penal, el

fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas (1)». *Diario La Ley* nº 8468, 28 de enero de 2015.

GARCÍA SÁNCHEZ, Manuel. «Retos de la computación en la nube» en MARTÍNEZ MARTÍNEZ RICARD (Editor), *Derecho y Cloud Computing.* Thomson Reuters- Aranzadi. Pamplona. 2012.

GARRIDO LORENZO, M. Ángeles. «Valoración en el juicio oral de la prueba y conexión de antijuridicidad». *Diario La Ley*, Nº 7573, 21 de Febrero de 2011. LA LEY 1829/2011.

GIL ANTÓN, Ana María. «El menor y la tutela de su entorno virtual a la luz de la reforma del Código Penal LO 1/2015. Virtual environment and child protection», *Revista de Derecho UNED*, núm. 16, 2015.

GINER DE LA FUENTE. Fernando. *Los sistemas de información en la sociedad del conocimiento*. ESIC. Madrid. 2004.

GIMENO SENDRA. Vicente. *Manual de Derecho Procesal Penal*. Colex- UNED. Madrid. 2014.

GIMENO SENDRA, Vicente. *Derecho Procesal Penal.* Segunda edición. Thomson Reuters Civitas. Pamplona. 2015.

GIMENO SENDRA, Vicente, MORENILLA ALARD, Pablo. TORRES DEL MORAL, Antonio, DÍAZ MARTÍNEZ, Manuel. *Los derechos fundamentales y su protección constitucional*. EDISOFER. Madrid. 2017.

GÓMEZ RIVERO, Mª del Carmen, «Principios limitadores del ius puniendi», en GÓMEZ RIVERO, Mª del Carmen (Dir), *Nociones fundamentales de Derecho Penal, Parte General.* Tecnos Madrid, 2015.

GONZÁLEZ CANO, M. Isabel y FIDALGO GALLARDO, Carlos. «Valoración de la prueba, presunción de inocencia y principio in dubio pro reo» en ROMERO PRADAS, M. Isabel (Dir) y GONZÁLEZ CANO, M. Isabel. *La Prueba. Tomo II. La prueba en el proceso penal*. Tirant lo Blanch. 2017.

GONZÁLEZ MONTES-SÁNCHEZ, José Luis. «Reflexiones sobre el proyecto de Ley Orgánica de modificación de la LECRIM para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica». *Revista electrónica de Ciencia Penal y criminología*. RECPC 17-06 (2015).

GUDIN RODRíGUEZ-MAGARIÑOS, Antonio Evaristo «La protección de datos en el tratamiento procesal de los dispositivos de almacenamiento masivo de información». *La Ley Penal*, Nº 125, Marzo-Abril 2017. LA LEY 3870/2017.

HOYOS SANCHO, Montserrat (Coord.). *El proceso penal en la Unión Europea: garantías esenciales*. Instituto de Estudios Europeos, Lex Nova. Valladolid. 2008.

IGARTUA SALAVERRÍA, Juan. *Valoración de la prueba, motivación y control en el proceso penal*. Tirant lo Blanch. Valencia 1995.

JIMÉNEZ SEGADO, Carmelo PUCHOL AIGUABELLA, Marta. «Las medidas de investigación tecnológica limitativas de los derechos a la intimidad, la imagen, el secreto de las comunicaciones y la protección datos». *Diario La Ley*, Nº 8676, Sección Doctrina, 7 de Enero de 2016. LA LEY.

JIMENO BULNES, Mar. «Orden europea de detención y entrega: garantías esenciales», en HOYOS SANCHO, Montserrat (Coord.). *El proceso penal en la Unión Europea: garantías esenciales.* Instituto de Estudios Europeos, Lex Nova. Valladolid. 2008.

JOÄO ANTUNES, María. *Código de processo penal.* Coimbra. Coimbra editora. 2001.

LADRÓN TABUENCA, Pilar. «Las intervenciones telefónicas en el ordenamiento jurídico español: visión jurisprudencial». *La Ley pena*l nº 4. Abril de 2004. La Ley 606/2004.

LÓPEZ-BARAJAS PEREA, Inmaculada. «Garantías constitucionales en la investigación tecnológica del delito: previsión legal y calidad de la ley». *Revista de Derecho Político UNED*, Nº 98. enero-abril 2017.

LÓPEZ-BARAJAS PEREA, Inmaculada. «Nuevas tecnologías aplicadas a la investigación penal: el registro de equipos informáticos». *Revista de Internet derecho y política*. IDP N.º 24 (Febrero, 2017).

LÓPEZ JIMÉNEZ, Raquel. «Régimen jurídico de los datos personales obtenidos en los descubrimientos casuales durante la investigación de los delitos» en COLOMER HERNÁNDEZ, Ignacio. (Dir) Cesión de datos personales y evidencias entre procesos penales y procedimeintos administrativos sancionadores o tributarios. Thomson Reuters Aranzadi. Pamplona 2017.

LÓPEZ ORTEGA, Juan José (Dir,). *El derecho a la intimidad. Nuevos y viejos debates*. Dykinson, Madrid. 2017.

LÓPEZ RAMÍREZ, Antonio. *La prueba ilícita penal*. Tirant lo Blanch. Ciudad de Méjico. 2019.

DE LUCAS MARTÍN, Ignacio. «La prueba en el proceso penal en el contexto de la Unión Europea», en HOYOS SANCHO, Montserrat (Coord). *El proceso penal en la Unión Europea: garantías esenciales*. Instituto de Estudios Europeos, Lex Nova. Valladolid. 2008.

MAGRO SERVET, Vicente. «Aspectos prácticos de la ejecución de las diligencias de investigación policial de intervención telefónica y de entrada y registro». *La Ley Penal*, Nº 65, Sección Estudios, Noviembre 2009. LA LEY 19958/2009.

MANRIQUE C. SÁNCHEZ. «La Guardia Civil introduce un infiltrado en una red internacional de pederastas por WhatsApp». *Diario El País*. Alicante 17 ENE 2018 - 13:56 CET.

MARCHENA GÓMEZ, Manuel; GONZÁLEZ CUÉLLAR SERRANO, Nicolás, *La reforma de la Ley de Enjuiciamiento Criminal en 2015*. Ediciones jurídicas Castillo de Luna. Madrid. 2015.

MARTÍN MARTÍN DE LA ESCALERA, A, M. «El registro de almacenamiento masivo de la información». Ponencias de Formación organizadas por la Fiscalía General del Estado. Jornadas de 27 de abril de 2016 tituladas “La interceptación de las Comunicaciones telefónicas y telemáticas”. Enlace:https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20Martín%20Martín%20de%20la%20Escalera,%20Ana%20Mª.pdf?idFile=bf66c357-e4d4-4701-8a4d-83d6c103ebe5.

MARTÍNEZ ARRIETA, Andrés. *El recurso de casación penal. Control de la presunción de inocencia.* Comares. Granada. 1996.

MARTÍNEZ MARTÍNEZ RICARD (Editor), *Derecho y Cloud Computing.* Thomson Reuters-Aranzadi. Pamplona. 2012.

MARTÍN MORALES, Joaquín. *El régimen constitucional del seguimiento directo de personas*. Comares. Granada. 2015.

DE MIGUEL ASENSIO, Pedro Alberto. «Aspectos internacionales de la protección de datos: las sentencias Schrems y Weltimmo del Tribunal de Justicia». *La Ley Unión Europea*, Nº 31, 30 de Noviembre de 2015.

MIRANDA ESTRAMPES, Manuel. *El concepto de prueba ilícita y su tratamiento en el proceso penal*. BOSCH. Barcelona. 2005.

MIRANDA WALLACE, Dennis. «Registro remoto de equipos informáticos. Comentario crítico al artículo 588 SEPTIES LECRIM». *Revista General de Derecho Procesal, nº* 42. 2017.

MIREILLE DELMAS MARTY y ASSOCIATION DE RECHERCHES PÉNALES EUROÉENNES (ARPE). *Procesos penales de Europa (Alemania, Inglaterra, País de Gales, Bélgica, Francia, Italia)*. Edijus. Zaragoza, 2000.

MONTERO AROCA, Juan. *Derecho jurisdiccional II. Proceso Civil.* Tirant lo Blanch. Valencia 2018.

MORENO CATENA, Víctor. *Derecho Procesal Penal*. Tirant lo Blanch. Valencia. 2019.

MUERZA ESPARZA, Julio. *Las reformas procesales penales de 2015. Nuevas medidas de agilización, de investigación y de fortalecimiento de garantías en la justicia penal.* Thomson Reuters Aranzadi, Navarra. 2015.

MÜLLER, FRIEDRICH. *La posibilidad de los derechos fundamentales: cuestiones para una dogmática práctica de los derechos fundamentales*. Dykinson. Madrid. 2016.

NADAL GÓMEZ, Irene. «El régimen de los hallazgos casuales en la Ley 13/2015, de modificación de la LECrim». *Revista General de Derecho Procesal*. nº 40. 2016.

NAVARRO MASSIP, Jorge, «El maquiavelismo probatorio de la prueba ilícitamente obtenida en el proceso penal», en *La prueba en el proceso penal,* Thomsom Reuters Aranzadi, Pamplona, 2016.

NEIRA PENA, Ana María. «La interceptación de las comunicaciones de la persona jurídica investigada». *Justicia: revista de derecho procesal*. Núm. 2. Año 2016.

NOYA FERREIRO, María Lourdes. «Presupuestos constitucionales de las medidas de intervención de las comunicaciones I». *Revista xuridica da Universidade de Santiago de Compostela*, Vol. 8, Nº 2, 1999.

DE LA OLIVA SANTOS, Andrés en *Derecho Procesal Penal*. Centro de Estudios Ramón Areces. Madrid. 2000.

ORTEGA GIMÉNEZ, Alfonso. «Cloud Computing. Protección de datos y Derecho internacional privado (resolución de controversias y determinación de la Ley aplicable)» en MARTÍNEZ MARTÍNEZ RICARD (Editor), *Derecho y Cloud Computing.* Thomson Reuters-Aranzadi. Pamplona. 2012

ORTÍZ PRADILLO, Juan Carlos. «Nuevas medidas tecnológicas de investigación criminal para la obtención de prueba electrónica», en ORTÍZ PRADILLO, Juan Carlos, *El proceso penal en la sociedad de la información. Las nuevas tecnologías para probar el delito*. Editorial La Ley, Madrid, 2012. La Ley 7959/2012.

ORTÍZ PRADILLO, Juan Carlos. *Problemas procesales de la ciberdelincuencia*. Colex. Madrid. 2013.

OTAMENDI ZOZAYA, Fermín. *Las últimas reformas de la Ley de Enjuiciamiento Criminal. Una visión práctica tras un año de vigencia*. Dykinson. Madrid. 2017.

PAZ RUBIO, José María, MENDOZA MUÑOZ, Julio, OLLE SESÉ, Manuel y RODRÍGUEZ MORICHE, Rosa María, *La prueba en el proceso penal. Su práctica ante los Tribunales*. Colex, Madrid, 1999.

PERANDONES ALARCÓN, Marta. «La recíproca limitación de los derechos fundamentales y la averiguación de la verdad en el proceso penal». *La Ley Penal*, Nº 117. Noviembre-Diciembre 2015. La Ley 7547-2015.

PERELLO DOMENECH, Isabel. «El principio de proporcionalidad y la jurisprudencia constitucional». *Revista Jueces para la Democracia*. Nº 28. 1997.

PEREZ LUÑO, Antonio E. *Los derechos fundamentales*. Tecnos. Madrid. 2005.

PÉREZ TREMPS, Pablo. *El recurso de amparo*. Tirant lo Blanch. Valencia. 2015.

PICÓ I JUNOY, Joan. «Nuevas perspectivas sobre el alcance anulatorio de las pruebas ilícitas». *Diario La Ley*, Sección Doctrina, 1997. LA LEY 11968/2001 I.

RICHARD GONZÁLEZ, Manuel. «Conductas susceptibles de ser intervenidas por medidas de investigación electrónica. Presupuestos para su autorización». *Diario La Ley*, Nº 8808, 21 de Julio de 2016. LA LEY 5735/2016 I.

RÍOS PINTADO, Juan Francisco. «La reforma procesal. Incorporación al proceso de los datos de tráfico; preservación específica de datos informáticos (arts. 588 ter j y 588 octies de la Ley de Enjuiciamiento Criminal)». Ponencias de formación realizadas por la Fiscalía general del Estado de 10 de marzo de 2016. Enlace: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20Rios%20Pintado.pdf?idFile=9bb2604a-0ca5-432c-8124-f51611957c7b

RIVES SEVA, Antonio Pablo. *La intervención de las comunicaciones en el proceso penal. Análisis doctrinal, legislación y jurisprudencia*. Bosch. Barcelona. 2010.

RODRÍGUEZ LAINZ, José Luis. *El secreto de las comunicaciones y su interceptación legal. Adaptado a la Ley Orgánica 13/2015, de reforma de la Ley de Enjuiciamiento Criminal*. Editorial Sepin, Madrid, 2016

RODRÍGUEZ LAINZ, José Luis. «¿Podría un juez español obligar a Apple a facilitar una puerta trasera para poder analizar información almacenada en un iPhone 6?». *Diario La Ley*, Nº 8729. LA LEY 1356/2016 I.

RODRÍGUEZ LAINZ, José Luis. «Tres cuestiones polémicas sobre el registro de dispositivos electrónicos de almacenamiento masivo de información». *BASE DOCTRINAL ED. SEPIN*. Nº DOCUMENTO SP/DOCT/21066. Septiembre 2016.

RODRÍGUEZ LAINZ, José Luis. «Sobre la naturaleza jurídica de los datos identificadores de aplicaciones de dispositivos de comunicaciones. Comentario a la STS, SALA 2.ª, 551/2016». *Diario La Ley*, Nº 8831, 26 de Septiembre de 2016. LA LEY 6777/2016.

RODRÍGUEZ LAINZ, José Luis, "Intervención judicial de comunicaciones vs. registro remoto sobre equipos informáticos: los puntos de fricción". *Diario La Ley*, Nº 8896, 9 de Enero de 2017. LA LEY 10072/2016.

RODRÍGUEZ LAINZ, José Luis. «Registro policial de dispositivos de almacenamiento masivo de datos por razones de urgencia. Comentario a la Sentencia del TEDH del caso Trabajo Rueda vs. España». *Revista Juridica editorial SEPIN*. SP/DOCT/22992.

RODRÍGUEZ LAINZ, José Luis. «Sobre la dimensión temporal de las medidas de investigación tecnológica». *Base doctrinal ED. SEPIN*. Nº Documento SP/DOCT/75471. Mayo 2018.

RODRÍGUEZ LAINZ, José Luis. «Registro de dispositivos de almacenamiento masivo de información». Comunicación presentada en el curso Ciberdelincuencia. Problemática penal de las redes sociales, celebrado en Valencia los días 9 y 10 de marzo de 2017. (Texto original no publicado).

RODRÍGUEZ LAINZ, José Luis, «Sobre la pretendida dimensión formal del derecho al entorno digital. (A propósito de la STS, Sala 2ª, 489/2018, de 23 de octubre)». SEPIN, Artículo Monográfico. Febrero 2019. *Base doctrinal ED. SEPIN*. Referencia: SP/DOCT/81702.

RODRÍGUEZ LAINZ, José Luis. «Alcance de la medida de ingerencia y resgistro de dispositivo de almacenamiento masivo de datos. Comentario a la STS, Sala Segunda, de lo penal, 14-10-19». *Base de datos SEPIN*. SP/SENT/1020974.SP/DOCT/84003. Diciembre 2019.

DE LA ROSA CORTINA, José Miguel. «Acceso a ordenadores, dispositivos electrónicos y sistemas de almacenamiento masivo de memoria. Acceso remoto. Acceso a la nube». Ponencia del

Curso sobre Intervención de las Comunicaciones Telemáticas, Centro de Estudios Jurídicos del Ministerio de Justicia. Madrid. 22 de mayo 2014. Enlace: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20escrita%20Sr%20de%20la%20Rosa%20Cortina%20(2).pdf?idFile=3d0616d9-3c76-4d41-9e37-de5c8ffcab78

RUBIO ALAMILLO, Javier. «La informática en la reforma de la Ley de Enjuiciamiento Criminal». *Diario La Ley*, Nº 8662, 10 de Diciembre de 2015. LA LEY 7030/2015.

SÁNCHEZ GONZÁLEZ, Santiago, *Dogmática y práctica de los derechos fundamentales*. Tirant lo Blanch. Valencia. 2015.

SANCHÍS CRESPO, Carolina. *La prueba por medios audiovisuales e instrumentos de archivo en la LEC 1/2000 (Doctrina, jurisprudencia y formularios)*. Tirant lo Blanch "abogacía práctica". Valencia. 2002.

SANCHÍS CRESPO, Carolina. *La prueba por soportes informáticos.* Tirant lo Blanch "abogacía práctica". Valencia.1999.

SANCHÍS CRESPO, Carolina. «Puesta al día de la instrucción penal: la interceptación de las comunicaciones telefónicas y telemáticas». *La Ley Penal* nº 125. Marzo-abril 2017. LA LEY 3914/2017.

SOLAR CALVO, Puerto. «La protección de datos en la UE: recapitulación de novedades». *Revista Aranzadi Unión Europea* núm. 1/2017.

SPANGHER Giorgio. *Codice de procedura penale*. G.GIAPPICHELLI EDITORE. TORINO. 2005.

TRENADO SEARA, Javier. «La ineficaz Orden Europea de Investigación en materia penal». *Revista Electrónica Abogacía Española*. 10 de noviembre de 2017.

VALVERDE MEGÍAS, Roberto. «Intervención de comunicaciones telemáticas y registro remoto». Ponencia realizada en los cursos de formación continuada realizados en fecha 27 de abril de 2016 bajo la denominación de *La interceptación de las comunicaciones telefónicas y telemáticas*.

Enlace:https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20Valverde%20Meg%C3%ADas,%20Roberto.pdf?idFile=c740b0e1-8842-4ef7-8983-23c4a0732291.

VELASCO NÚÑEZ, Eloy, «Investigación procesal penal en redes, terminales, dispositivos informáticos, imágenes, GPS, balizas: la prueba tecnológica». *Diario la Ley*, nº 8183, 4 de noviembre de 2013. La ley 8334/2013.

VELASCO NÚÑEZ, Eloy. «Investigación tecnológica de delitos: disposiciones comunes e interceptaciones telefónicas y telemáticas». Ponencias de formación. Jornadas de 10 de marzo de 2016 tituladas "Jornadas de especialistas en criminalidad informática". Enlace: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20Velasco%20Nuñez,%20Eloy.pdf?idFile=7b2fdf75-4a93-41bd-9adc-fe3042c95cc0.

ZOCO ZABALA, Cristina. *Nuevas tecnologías y control de las comunicaciones*. Thomson Reuters - Aranzadi. Navarra. 2015.

ZUBIRI DE SALINAS, Fernando. «¿Qué es la sana crítica. La valoración judicial del Dictamen de experto». *Revista de Jueces para la democracia información y debate*. nº 50, año 2004.